DIKLAT TEKNIS SUBSTANTIF SPESIALISASI
OPERATOR CONSOLE

MODUL

TATA KELOLA TEKNOLOGI KOMUNIKASI DAN INFORMASI (TIK)

oleh:

Mohammad Djufri
Widyaiswara Ahli Madya Pusdiklat Pajak

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
BADAN PENDIDIKAN DAN PELATIHAN KEUANGAN
PUSDIKLAT PAJAK
2017

KATA PENGANTAR

Alhamdulillah, segala puji syukur bagi Allah SWT atas segala rahmat-Nya Modul ini dapat diselesaikan. Modul Tata Kelola TIK ini dapat dipergunakan sebagai salah satu Modul untuk DTSS Administrator TIK dan DTSS Manajemen Data dan Informasi yang diselenggarakan oleh Pusdiklat Pajak. Modul ini juga dapat digunakan untuk DTSD Pajak I dan DTSD Pajak II.

Para peserta diklat dapat dari berbagai kalangan yang berminat pada hal ini, khususnya para Admin TIK dan para Kepala Seksi Pengolahan Data dan Informasi Direktorat Jenderal Pajak.

Dalam Modul ini dijelaskan secara ringkas tiga pokok bahasan, yaitu yang pertama adalah Cetak Biru TIK DJP, Tata Kelola TIK DJP, dan Pengetahuan Organisasi dan Tata Laksana Organisasi TIK.

Diharapkan para peserta diklat mendapatkan pemahaman secara umum tentang Modul ini.

Terima kasih Penulis sampaikan kepada :

1. Kepala Pusdikat Pajak beserta staf yang memfasiltasi kegiatan penulisan Modul ini;
2. Rekan-rekan dari Direktorat Transformasi Teknologi Komunikasi dan Informasi dan Direktorat Teknologi dan Informasi Perpajakan Direktorat Jenderal Pajak yang banyak memberi sumbang saran dan pemikiran sebagai bahan Modul ini;
3. Rekan-rekan widyaiswara yang memberi support untuk menyelesaikan Modul ini.

Harapan Penulis agar Modul ini dapat bermanfaat bagi peserta diklat dan dapat diimplementasikan pada pekerjaannya sehari-hari.

Jakarta, September 2017

Penyusun,

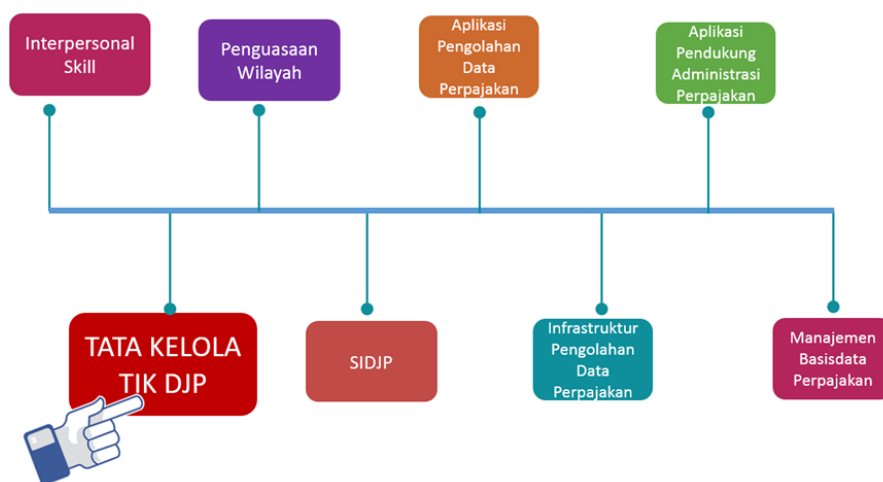
Mohammad Djufri

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

PETUNJUK PENGGUNAAN MODUL

Modul Tata Kelola TIK ini merupakan satu dari delapan modul yang saling melengkapi yang digunakan untuk Diklat Teknis Substantif Spesialis (DTSS) Administrator TIK. Modul ini dapat juga digunakan untuk DTSS Manajemen Data dan Informasi yang diikuti para Kepala Seksi Pengolahan Data dan Informasi (PDI) Direktorat Jenderal Pajak.

Untuk memudahkan mempelajari isi modul ini, peserta diklat dapat melakukan hal-hal sebagai berikut :

1. Pelajari dan pahami uraian serta contoh masing-masing kegiatan belajar yang ada, dimulai dari Kegiatan Belajar pertama hingga Kegiatan belajar terakhir secara sistematis.
2. Setelah uraian dan contoh di pelajari di ikuti dengan latihan dan test formatif, apabila hasil dari test formatif ini diatas 80%, maka dapat melanjutkan ke kegiatan belajar berikutnya, jika belum maka sebaiknya diulangi dahulu sampai benar-benar dapat dipahami.
3. Setelah semua kegiatan belajar selesai dipelajari, maka peserta diharapkan untuk menjawab test sumatif di akhir modul ini untuk memastikan tingkat penguasaaannya.

KEDUDUKAN MODUL DALAM DIKLAT

PETA KONSEP

1. Tujuan Penyusunan
2. Arah Dan Batasan Pengembangan TIK
3. Layanan TIK yang Diharapkan
4. Aplikasi yang Diharapkan
5. Infrastruktur yang Diharapkan
6. Analisis Kesenjangan Aplikasi
7. Analisis Kesenjangan Infrastruktur
8. Roadmap TIK

1. Latar Belakang Tata Kelola TIK
2. Kebijakan Tata Kelola TIK DJP
3. Kebijakan Pengelolaan Keamanan Informasi
4. Kebijakan Pengelolaan Layanan TIK

1. Organisasi TIK DJP
2. Proses Bisnis TIK DJP

PENDAHULUAN

1. Deskripsi Singkat

Modul Tata Kelola TIK ini memuat materi pelajaran tentang kompetensi yang harus dimiliki oleh para Adiministrator TIK Direktorat Jenderal Pajak, khususnya kompetensi dalam memahami tata kelola TIK di DJP. Modul ini meliputi: (1) Cetak Biru TIK yang membahas arah kebijakan TIK DJP ke depan; (2) Tata Kelola TIK DJP, yang membahas kebijakan dalam melakukan tata kelola TIK DJP sesuai proses bisnis DJP; dan (3) Pengetahuan Organisasi dan Tata Laksana TIK DJP, yang membahas bagaimana organisasi DJP yang berkaitan dengan tata kelola TIK serta bagaimana proses bisnis TIK DJP.

2. Prasyarat Kompetensi

Prasyarat kompetensi yang diperlukan untuk dapat mempelajari modul ini adalah peserta diklat adalah pegawai DJP yang akan diangkat menjadi Admin TIK atau sudah menduduki posisi Admin TIK paling lama satu tahun.

3. Standar Kompetensi (SK) dan Kompetensi Dasar (KD)

3.1. Standar Kompetensi

Setelah mengikuti pembelajaran ini, Peserta diklat mampu mempraktikkan tata kelola TIK sesuai kewenangannya dan sesuai dengan ketentuan mengenai Tata Kelola TIK DJP yang berlaku.

3.2. Kompetensi Dasar

Setelah mengikuti pembelajaran ini Peserta mampu:

a. Memahami cetak biru TIK DJP sesuai dengan ketentuan yang berlaku.
b. mempraktikkan tata kelola TIK sesuai kewenangannya dan sesuai dengan ketentuan yang berlaku.
c. Memahami Pengetahuan Organisasi dan Tata Laksana TIK DJP sesuai dengan ketentuan yang berlaku.

4. Relevansi Modul

Modul ini berguna sumber informasi/pengetahuan bagi yang ingin mengetahui bagaimana tata Kelola TIK dilaksanakan di DJP sekaligus sebagai panduan dalam melakukan tata kelola TIK dengan benar sesuai ketentuan di unit organisasi masing-masing.

.

CETAK BIRU TIK DJP

1. Indikator

Setelah mengikuti pembelajaran, peserta diklat mampu :

☑ memahami tujuan penyusunan Cetak Biru TIK DJP

☑ memahami arah dan batasan pengembangan TIK

☑ memahami *roadmap* TIK

Dalam dunia arsitektur, istilah *blue print* atau cetak biru sudah sangat lazim digunakan. Sesuai dengan namanya, cetak biru dalah dokumen dengan kertas berwarna biru yang digunakan sebagai referensi atau acuan utama dalam proses pembangunan rumah atau gedung yang direncanakan. Mengadopsi istilah yang sama, bidang Teknologi Informasi dan Komunikasi (TIK) pun mengenal istilah cetak biru sebagai acuan jangka panjang dalam perencanaan, pengembangan, pengoperasian, dan pemeliharaan layanan berbasis TIK beserta komponen teknologi pendukungnya dalam bentuk dokumen Cetak Biru TIK (CBTIK). CBTIK merupakan dokumen resmi Direktorat Jenderal Pajak (DJP) yang digunakan sebagai acuan utama dalam merencanakan, mengembangkan, mengoperasikan, dan memelihara layanan TIK di DJP dari tahun 2015 hingga tahun 2019.

2. Tujuan Penyusunan

CBTIK DJP 2015-2019 disusun sedemikian rupa untuk mencapai tujuan-tujuan tertentu, yaitu:

a. Menjamin keselarasan (*alignment*) antara sasaran strategis TIK dengan sasaran strategis DJP.

b. Memberikan kesamaan pemahaman, keserentakan tindak, dan keterpaduan langkah-langkah Unit Kerja TIK DJP dalam pelaksanaan kebijakan dan strategi pengembangan TIK secara menyeluruh.
c. Menjadi acuan perencanaan seluruh kegiatan TIK di DJP dengan memperhatikan kepatuhan pada prinsip-prinsip yang harus dilaksanakan dan program-program yang telah ditetapkan.
d. Menjadi acuan perencanaan sumber daya yang diperlukan untuk melaksanakan seluruh kegiatan TIK di DJP.
e. Menjadi instrumen strategis *Board of Directors* (BoD) untuk memastikan akuntabilitas pelaksanaan kegiatan TIK, mengendalikan investasi TIK, dan memastikan perolehan manfaat investasi TIK yang dilakukan.

1. Pilar-Pilar Pengembangan TIK

Untuk mencapai sasaran-sasaran strategis TIK, pengembangan TIK di DJP harus dilakukan secara terarah sehingga fokus pengembangan TIK di DJP pun jelas dan dapat berjalan secara efektif dan efisien. Arah pengembangan TIK tersebut dituangkan dalam Pilar-Pilar Pengembangan TIK.

Pilar-pilar pengembangan TIK adalah panduan mengenai arah pengembangan TIK di DJP sehingga DJP dapat menentukan teknologi yang digunakan atau diterapkan dalam pengembangan TIK, baik dari sisi aplikasi, data, maupun infrastruktur selama lima tahun mendatang. Pilar-pilar tersebut adalah *Social Business*, *Mobile*, *Cloud Computing*, dan *Big Data Analytics*.

1.1. Social Business

Pilar *Social Business* mengarahkan pengembangan TIK di DJP untuk membantu menggali perilaku dan kebiasaan hidup masyarakat secara komprehensif. Contoh yang paling sederhana adalah dengan mengambil informasi yang tersedia di berbagai media sosial untuk mencari tahu perilaku belanja, kebiasaan berlibur, dan berbagai sisi lain dalam kehidupan masyarakat yang relevan dengan proses penggalian potensi pajak. Pada intinya, pilar *Social Business* ini menegaskan bahwa data dan informasi yang dibutuhkan oleh DJP tidak lagi terbatas pada sumber-sumber yang formal, tapi juga mencakup berbagai sumber informasi informal yang dapat diandalkan untuk menggali potensi pajak.

1.2. Mobility

Pilar *Mobility* mengarahkan pengembangan TIK di DJP untuk memiliki jangkauan yang lebih luas, khususnya terhadap anggota masyarakat yang lebih leluasa menggunakan perangkat *mobile* atau anggota masyarakat yang pilihannya terbatas pada perangkat *mobile*. Pilar *Mobility* juga mengarahkan pengembangan TIK di DJP untuk berorientasi pada layanan *mobile-first*, yaitu aplikasi atau sistem informasi yang sejak awal dirancang untuk diakses melalui perangkat *mobile*, baik oleh WP maupun oleh pengguna di internal DJP. Dengan begitu, pilar *Mobility* akan mengarahkan pengembangan TIK di DJP untuk mendukung terwujudnya layanan kepada WP yang tidak dibatasi ruang dan waktu.

1.3. Cloud Computing

Pilar *Cloud Computing* mengarahkan pengembangan TIK di DJP untuk menjadi fleksibel dalam pengelolaan infrastruktur TIK, yaitu dengan menyerahkan tanggung jawab pengelolaan infrastruktur TIK tersebut ke penyedia layanan *cloud computing*. Pilar tersebut mengarahkan pengembangan TIK di DJP menjadi *agile* (mudah beradaptasi terhadap perubahan) untuk memenuhi kebutuhan infrastruktur TIK sehingga ketersediaan layanan TIK pun menjadi optimal. Sifat *agile* tersebut juga diterapkan dalam pengembangan aplikasi atau sistem informasi di DJP sehingga ketersediaan layanan TIK di DJP dari hulu ke hilir dapat dengan mudah beradaptasi terhadap perubahan kebutuhan.

1.4. Big Data Analytics

Analytics merupakan proses yang tidak terpisahkan dari DJP, khususnya dalam penggalian potensi pajak dan pencegahan penggelapan pajak. Pencanangan pilar *Big Data Analytics* bertujuan untuk memperkuat proses *analytics* yang sudah dilakukan di DJP dengan menyediakan dan memanfaatkan *big data*, baik yang bersifat terstruktur, seperti basis data, maupun tidak terstruktur, seperti data dari berbagai media sosial atau dari sumber data eksternal (pihak ketiga). Dengan memperkuat *analytics* melalui pemanfaatan *big data*, semakin banyak pola dan korelasi yang dapat ditemukan di dalam data perpajakan

sehingga keberhasilan proses penggalian potensi pajak dan pencegahan penggelapan pajak pun semakin tinggi.

Dari keempat pilar pengembangan TIK khususnya menyangkut aplikasi, dirumuskan beberapa aplikasi yang akan dikembangkan sebagaimana Tabel 1.1 berikut.

Tabel 1.1 McFarlan Strategic Grid untuk Aplikasi yang Diharapkan

Strategic	High Potential
Analytics Dashboard & Reporting Data Quality	Compliance Risk Management
Key Operational	Support
SIDJP NINE TPT Online Approweb Taxpayer Account e-Registration e-Billing (MPN G2) Cash Receipt System e-Faktur e-Filing e-SPT e-Form Geotagging	Tax Clearance Website & Mobile App Call Center SIKKA Internal Support Data and Information Exchange ETL Document Management Project Management Knowledge Management

a. High Potential.

Aplikasi-aplikasi yang masuk ke dalam kuadran *high potential* adalah aplikasi-aplikasi yang memiliki potensi untuk meningkatkan penerimaan pajak, tapi potensi itu sendiri belum terbukti. Berdasarkan hasil pemetaan di atas, hanya ada 1 aplikasi yang masuk ke dalam kuadran *high potential*, yaitu: *Compliance Risk Management*.

Compliance Risk Management merupakan aplikasi yang digunakan untuk melakukan pengawasan berbasis risiko. Aplikasi ini dapat digunakan untuk menampilkan besarnya risiko kepatuhan WP. Besarnya risiko tersebut dapat

digunakan sebagai acuan untuk menentukan para WP yang perlu diawasi oleh DJP. Dengan begitu, langkah-langkah pengawasan menjadi lebih tepat karena dapat diarahkan kepada para WP dengan risiko kepatuhan yang tinggi.

b. Strategic.

Aplikasi-aplikasi yang masuk ke dalam kuadran *strategic* adalah aplikasi-aplikasi yang dapat mengubah arah kebijakan dan kegiatan operasional di dalam lingkungan DJP dengan tujuan untuk mengoptimalkan penerimaan pajak. Aplikasi-aplikasi *strategic* bagi DJP adalah:

1) *Analytics.*

Analytics mencakup aplikasi-aplikasi yang digunakan untuk melakukan analisis terhadap data. Analisis data yang dilakukan dengan menggunakan *Analytics* umumnya dilakukan untuk mengidentifikasi pola-pola tertentu di dalam data terkait. Salah satu contohnya adalah aplikasi *data mining* yang dapat digunakan untuk melakukan analisis terhadap data perpajakan sehingga dapat mengidentifikasi pola *tax evasion* atau *tax avoidance*.

2) *Dashboard & Reporting.*

Dashboard mencakup aplikasi-aplikasi yang digunakan untuk menampilkan sebaran dan agregat data perpajakan yang dapat digunakan sebagai bahan pengambilan keputusan seperti akumulasi penerimaan pajak, hasil pemeriksaan pajak, atau hasil penyidikan pajak. Informasi yang tersedia di dalam *Dashboard* dapat diakses dalam bentuk yang lebih spesifik atau data yang lebih rinci melalui berbagai aplikasi *Reporting*. Dengan begitu, informasi yang diperlukan oleh para pengambil keputusan dapat diperoleh secara komprehensif.

3) *Data Quality.*

Data Quality mencakup aplikasi-aplikasi yang digunakan untuk menjamin kualitas data perpajakan, khususnya kualitas data yang diperoleh dari pihak ketiga. Aplikasi-aplikasi tersebut secara spesifik digunakan untuk menentukan NPWP yang sesuai bagi setiap data yang diperoleh dari pihak ketiga. Dengan begitu, data yang diperoleh dari pihak ketiga dapat dihubungkan dengan data WP yang tepat.

c. Key Operational.

Aplikasi-aplikasi yang masuk ke dalam kuadran *key operational* adalah aplikasi-aplikasi yang harus ada (*mandatory*) untuk menjalankan proses bisnis utama di dalam lingkungan DJP secara efektif dan efisien. Aplikasi-aplikasi *key operational* bagi DJP adalah:

1) *SIDJP NINE.*

SIDJP atau Sistem Informasi DJP *New Improved Novelty Excellence* (NINE) adalah aplikasi yang digunakan untuk mendukung jalannya berbagai proses bisnis di dalam lingkungan DJP, yaitu: Pendaftaran, Pembayaran, Pelaporan, Pengawasan, Pemeriksaan & Penyidikan, Penagihan, Keberatan & Banding, Pelayanan, Ekstensifikasi, PAP3D, *Accounting* & *Reporting*, *General Ledger*, *Compliance Performance System*.

2) *TPT Online.*

TPT Online adalah aplikasi yang digunakan oleh Petugas TPT di KPP dan Petugas KP2KP untuk menerima permohonan dan pelaporan WP di mana *database*-nya tersentralisasi di *Data Center* DJP sehingga data yang diakses adalah data yang *Real Time.*

3) *Approweb.*

Approweb adalah aplikasi yang digunakan oleh pegawai DJP, khususnya *Account Representative*, untuk mengakses profil WP. Aplikasi ini memiliki peran penting untuk melakukan penggalian potensi pajak dari WP terdaftar.

4) *Taxpayer Account.*

Taxpayer Account adalah aplikasi yang digunakan oleh WP untuk mengakses data perpajakannya sendiri seperti riwayat aktivitas pembayaran pajak, riwayat aktivitas pelaporan SPT, hutang pajak, atau piutang pajak.

5) *e-Registration.*

e-Registration adalah aplikasi administrasi data WP. Aplikasi ini digunakan untuk merekam permohonan WP terkait data dan statusnya (misalnya pendaftaran, pengukuhan PKP, perubahan data, pemindahan) maupun merekam

hasil penelitian dan pemeriksaan yang berkaitan dengan status dan data WP. Aplikasi ini diakses oleh WP melalui *channel* internet dan diakses oleh Seksi Pelayanan, Seksi Ekstensifikasi dan Penilaian dan Seksi Bimbingan Pendaftaran melalui intranet.

6) *e-Billing (MPN G2).*

Modul Penerimaan Negara Generasi 2 (MPN G2) merupakan sebuah ekosistem aplikasi *billing* yang memungkinkan proses pembayaran pajak dan sumber pemasukan negara lainnya dilakukan tanpa memerlukan proses rekonsiliasi. Salah satu aplikasi *billing* di dalam ekosistem tersebut adalah aplikasi e-Billing dari DJP. e-Billing adalah aplikasi *billing* berbasis *web* yang dapat digunakan oleh WP untuk melakukan aktivitas pembayaran pajak secara *online*. WP akan menggunakan aplikasi tersebut untuk membuat ID *billing*. Setelah itu, WP dapat membayar tagihan pajak terkait berdasarkan ID *billing* tersebut melalui *teller,* ATM, mini ATM (mesin EDC yang tersedia di KPP), atau melalui *Internet banking*. Dengan begitu, WP dapat membuat ID *billing* dan membayar tagihan pajak terkait kapan saja dan di mana saja serta mengurangi kesalahan rekam yang sebelumnya dilakukan oleh Bank atau Kantor Pos.

7) *Cash Receipt System.*

Cash Receipt System adalah aplikasi yang terpasang di mesin-mesin kasir dan mesin-mesin EDC untuk mendeteksi berbagai transaksi yang dilakukan oleh WP.

8) *e-Faktur.*

e-Faktur adalah aplikasi yang digunakan oleh para PKP untuk membuat faktur pajak dalam bentuk elektronik dengan penomoran dan dokumen faktur sepenuhnya diatur oleh DJP.

9) *e-Filing.*

e-*Filing* adalah aplikasi yang digunakan oleh WP untuk melaporkan SPT dalam bentuk elektronik secara *online*.

10) *e-SPT.*

e-SPT adalah aplikasi yang digunakan oleh WP untuk melaporkan SPT dalam bentuk elektronik. Bagian yang tidak terpisahkan dari aplikasi e-SPT ini adalah e-Withholding Tax, yaitu aplikasi yang digunakan oleh para pemotong pajak untuk membuat bukti potong pajak dalam bentuk elektronik dengan dokumen bukti potong pajak sepenuhnya diatur oleh DJP. Bukti potong pajak dalam bentuk elektronik itu dapat dilaporkan secara otomatis lewat aplikasi e-SPT.

11) *e-Form.*

e-Form adalah aplikasi yang digunakan untuk mengelola berbagai formulir yang dilaporkan oleh WP, seperti formulir SPT, formulir permohonan keberatan, atau formulir non-keberatan. Formulir-formulir tersebut tersedia dalam format PDF yang dapat diisi langsung. Isian tersebut akan disimpan dalam format QR Code sehingga dapat dibaca langsung oleh aplikasi e-Form. Dengan begitu, formulir yang dilaporkan oleh WP dapat langsung disimpan ke dalam basis data DJP tanpa perlu melewati proses perekaman secara manual.

12) *Geotagging.*

Geotagging adalah aplikasi yang digunakan oleh petugas pajak untuk menandai lokasi objek pajak, tempat usaha, atau merk yang dimiliki WP.

d. Support.

Aplikasi-aplikasi yang masuk ke dalam kuadran *support* adalah aplikasi-aplikasi yang digunakan untuk meningkatkan efektivitas dan efisiensi dari berbagai kegiatan operasional di dalam lingkungan DJP secara umum, tapi keberadaan aplikasi-aplikasi tersebut tidak menjadi keharusan. Aplikasi-aplikasi *support* bagi DJP adalah:

1) *Tax Clearance.*

Tax Clearance adalah aplikasi yang digunakan oleh pegawai DJP dan pihak ketiga yang diberikan ijin oleh DJP untuk memeriksa NPWP, pelaporan SPT, pembayaran pajak, ataupun pelunasan tunggakan pajak WP. Fungsi-fungsi yang tersedia pada aplikasi tersebut dapat mempermudah proses pemeriksaan

kewajiban perpajakan untuk WP terkait. Dengan begitu, proses untuk memperoleh keterangan bebas fiskal bagi WP pun menjadi lebih efisien.

2) *Website & Mobile App.*

Website resmi DJP digunakan sebagai sarana komunikasi antara DJP dan WP yang dapat diakses dengan baik lewat *web browser* di PC dan *mobile device* atau lewat aplikasi *native* di *mobile device*.

3) *Call Center.*

Call Center mencakup aplikasi-aplikasi yang digunakan untuk mengelola hubungan dengan WP misalnya menerima pengaduan WP, memberikan konsultasi WP, atau kegiatan lainnya dalam rangka melakukan meningkatkan kepuasan WP.

4) SIKKA.

SIKKA mencakup aplikasi-aplikasi yang digunakan untuk mengelola data pegawai, termasuk keuangan dan aset pegawai terkait. Selain itu, aplikasi ini juga memuat data kegiatan di dalam DJP sehingga dapat digunakan untuk menyebarluaskan informasi kegiatan yang relevan dengan pegawai yang mengaksesnya.

5) *Internal Support.*

Internal Support mencakup aplikasi-aplikasi yang digunakan untuk melaporkan dan menindaklanjuti keluhan yang terkait dengan SIDJP NINE dan aplikasi lainnya dari para pegawai DJP.

6) *Data & Information Exchange.*

Data & Information Exchange mencakup aplikasi-aplikasi yang digunakan untuk melakukan pertukaran data dengan pihak ketiga yang sudah bekerja sama dengan DJP dan dengan negara mitra Perjanjian Penghindaran Pajak Berganda (P3B).

7) ETL.

ETL atau *Extract-Transform-Load* mencakup aplikasi-aplikasi yang digunakan untuk mengolah berbagai data yang bersifat transaksional dari satu bentuk ke bentuk lain atau untuk mengolah data transaksional tersebut ke dalam bentuk ringkasan atau agregat. Aplikasi ini sangat dibutuhkan untuk meningkatkan efisiensi dan efektivitas pembuatan *enterprise data warehouse* di DJP.

8) *Document Management.*

Document Management mencakup aplikasi-aplikasi yang digunakan untuk mengelola berbagai dokumen perpajakan secara fisik dan elektronik, baik SPT, produk-produk hukum pajak, maupun dokumen-dokumen pendukung lainnya.

9) *Project Management.*

Project Management mencakup aplikasi-aplikasi yang digunakan untuk mengelola proyek, baik proyek TI maupun non-TI. Aplikasi-aplikasi tersebut diperlukan untuk mendeteksi kemungkinan terjadinya kegagalan dalam proyek sehingga keberhasilan proyek lebih terjamin. Khusus untuk proyek TI, aplikasi-aplikasi tersebut harus mengakomodasi 2 metodologi yang dikenal secara luas, yaitu *waterfall* dan *agile*.

10) *Knowledge Management.*

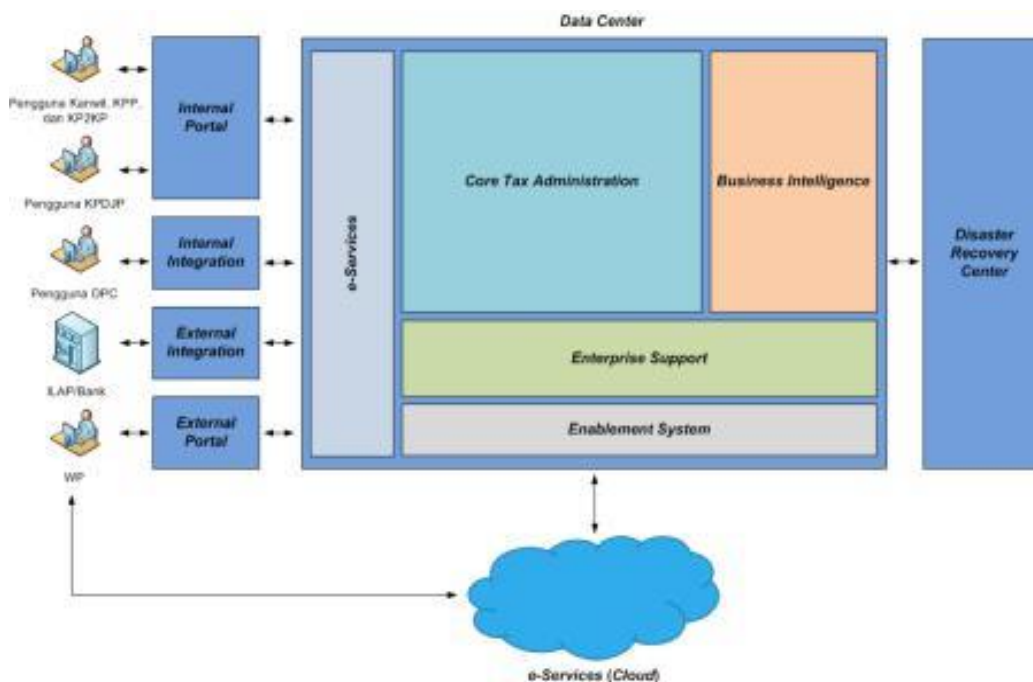
Knowledge Management mencakup aplikasi-aplikasi yang digunakan untuk menyimpan, mengelola, dan berbagi pengetahuan antara para pegawai DJP. Bagian-bagian pengetahuan yang bersifat umum (tidak bersifat terbatas untuk lingkungan internal) dapat dipublikasikan ke WP, misalnya yang terkait dengan produk-produk hukum pajak.

Sementara, dari sisi infrastruktur yang akan dikembangkan, mencakup tiga komponen infrastruktur TI yang perlu disediakan untuk menunjang jalannya berbagai aplikasi yang diharapkan DJP, yaitu *Data Center* (DC), *Disaster Recovery Center* (DRC), dan *Cloud*. DC merupakan infrastruktur TI utama yang menunjang aplikasi-aplikasi yang akan digunakan oleh para pegawai DJP, sementara DRC berfungsi sebagai cadangan DC.

Sangat penting bagi DJP untuk memiliki DRC dengan kapasitas dan konfigurasi yang sama dengan DC agar setiap aplikasi dan data yang terpasang

di dalam DC dapat dibuat cadangannya di dalam DRC. Sementara itu, *Cloud* akan menunjang aplikasi-aplikasi yang perlu diakses oleh WP. Beban kepemilikan dan pengelolaan infrastruktur TI DJP serta tanggung jawab terkait ketersediaan aplikasi dan layanan yang digunakan oleh WP akan menjadi tanggung jawab penyedia layanan *Cloud*. Cadangan dari setiap aplikasi dan data yang terpasang di dalam *Cloud* pun akan menjadi tanggung jawab penuh penyedia layanan *Cloud*.

Berikut ini adalah gambaran umum arsitektur TI yang diharapkan DJP, yang terbentuk dari komponen *Data Center* (DC), *Disaster Recovery Center* (DRC), dan *Cloud*.

Gambar 1.1 Gambaran Umum Arsitektur TI yang Diharapkan

2. Roadmap TIK

DJP perlu membuat perubahan-perubahan untuk mencapai kondisi TIK yang diharapkan. Perubahan-perubahan tersebut perlu dilakukan untuk mendukung sasaran-sasaran strategis TIK, khususnya “Pengembangan Sistem Informasi yang Terpadu” (TIK 4), “Peningkatan Ketersediaan Data dan Informasi yang lengkap dan berkualitas” (TIK 5), dan “Peningkatan Kualitas Layanan TIK” (TIK 6). Perubahan-perubahan tersebut perlu dilakukan untuk mendukung sasaran-

sasaran strategis TIK, yang diwujudkan melalui program-program terkait TIK yang dituangkan dalam bentuk *Roadmap* sebagaimana Tabel 1.2 dan Tabel 1.3.

Tabel 1.2 *Roadmap* Pengembangan Aplikasi 2015-2019

No.	Nama Program	2015	2016	2017	2018	2019
TIK 4: Pengembangan Sistem Informasi yang Terpadu						
1.	Pengembangan *Compliance Risk Management*	■	■	■	■	■
2.	Pengembangan SIDJP NINE	■	■	■	■	■
3.	Pengembangan TPT *Online*		■	■		
4.	Pengembangan *Taxpayer Account*		■	■		
5.	Pengembangan e-Billing (MPN G2)	■	■	■	■	■
6.	Pengembangan *Cash Receipt System*	■	■	■	■	■
7.	Pengembangan e-Faktur	■	■	■	■	■
8.	Pengembangan e-Filing	■	■	■	■	■
9.	Pengembangan e-SPT	■	■	■	■	
10.	Pengembangan e-Form		■	■		
11.	Pengembangan Aplikasi Geotagging	■	■			
12.	Pengembangan Aplikasi *Tax Clearance*	■	■			
TIK 5: Peningkatan Ketersediaan Data dan Informasi yang lengkap dan berkualitas						
1.	Pengembangan *Platform Analytics*		■	■	■	■
2.	Pengembangan *Platform Dashboard & Reporting*		■	■	■	■
3.	Pengembangan *Platform Data Quality*		■	■	■	■
4.	Pengembangan Aplikasi *Data & Information Exchange*	■	■	■	■	■
5.	Pengembangan *Document Management System*	■	■	■	■	
TIK 6: Peningkatan Kualitas Layanan TIK						
1.	Pengembangan *Website & Mobile App*	■	■	■	■	■
2.	Pengembangan *Project Management System*		■	■		
3.	Pengembangan *Knowledge Management System*		■	■		

Tabel 1.3 *Roadmap* Pengembangan Infrastruktur TIK 2015-2019

No.	Nama Program	2015	2016	2017	2018	2019
TIK 5: Peningkatan Ketersediaan Data dan Informasi yang lengkap dan berkualitas						
6.	Pengembangan *Master Data Management*	■	■	■	■	■
7.	Pengembangan *Enterprise Data Warehouse*	■	■	■	■	■
TIK 6: Peningkatan Kualitas Layanan TIK						
4.	Penerapan *Cloud Computing*		■	■	■	■
5.	Sinkronisasi DC-DRC	■	■	■	■	■

3. Latihan

a. Jelaskan tujuan dibuatnya Cetak Biru TIK DJP 2015-2019 !
b. Jelaskan arah pengembangan TIK DJP ke depan !
c. Jelaskan aplikasi yang diharapkan ke depannya oleh DJP !
d. Jelaskan arsitektur TI yang diharapkan ke depannya oleh DJP !
e. Menurut saudara sebagai *user*, apa yang paling *urgent* harus segera disiapkan oleh DJP?

4. Rangkuman

Peranan teknologi informasi dan komunikasi akan semakin meningkat seiring perkembangan jaman dan hingga akhirnya menjadi kebutuhan dalam setiap organisasi, tidak terkecuali DJP. Untuk itu, DJP telah membuat Cetak Biru 2015-2019 sebagai acuan jangka panjang dalam perencanaan, pengembangan, pengoperasian, dan pemeliharaan layanan berbasis TIK beserta komponen teknologi pendukungnya dalam rentang waktu 2015 hingga 2019. Arah kebijakan pengembangan TIK DJP dituangkan dalam empat Pilar Pengembangan TIK, yaitu *Social Business*, *Mobile*, *Cloud Computing*, dan *Big Data Analytics.* Dengan berdasar keempat Pilar Pengembangan TIK tersebut dirumuskan beberapa aplikasi yang akan dikembangkan dan arsitektur TI yang diharapkan.

5. Tes Formatif 1

Pilihlah jawaban yang paling tepat !

1. Salah satu tujuan dibuatnya Cetak Biru TIK DJP adalah :
   a) Sebagai pertanggungjawaban kepada stackholder khususnya stackholder penyandang dana pengembangan TIK
   b) Menyesuaikan dengan perkembangan jaman yang mengarah kepada penggunaan TIK
   c) Menjadi instrumen strategis *Board of Directors* (BoD) untuk mengambil keputusan terkait TIK
   d) Agar semua sumber daya DJP memahami TIK dalam mendukung pekerjaannya.

2. Arah pengembangan TIK dituangkan dalam empat Pilar Pengembangan TIK, yaitu :
   a) *Media Social* – High Technology - *Cloud Computing* - *Big Data Analytics*
   b) *Social Business* – *Mobile* - *Cloud Computing* - *Statistics*
   c) *Social Business* – *Mobile* – High Technology - *Statistics*
   d) *Social Business* – *Mobile* - *Cloud Computing* - *Big Data Analytics*

3. Data dan informasi yang dibutuhkan oleh DJP tidak lagi terbatas pada sumber-sumber yang formal, tapi juga mencakup berbagai sumber informasi informal yang dapat diandalkan untuk menggali potensi pajak. Pernyataan tersebut adalah prinsip pilar pengembangan TIK…
   a) *Social Business*
   b) *Mobility*
   c) *Cloud Computing*
   d) *Statistics*

4. Pengembangan TIK di DJP menjadi mudah beradaptasi terhadap perubahan khususnya untuk memenuhi kebutuhan infrastruktur TIK. Pernyataan tersebut adalah prinsip pilar pengembangan TIK…
   a) *Social Business*
   b) *Mobility*
   c) *Cloud Computing*
   d) *Statistics*

5 Aplikasi yang diharapkan oleh DJP dirumuskan sedemikian rupa berdasarkan McFarlan Strategic Grid, yang dikelompokkan dalam …
   a) High Potential- Strategic- Key Operational – Support
   b) High Potential- Main Strategic- Key Strategic – Support Strategic
   c) High Potential- Main Strategic- Key Operational – Support
   d) High Potential- Main Strategic- Key Strategic – Support

6. Aplikasi yang tergolong High Potential adalah…
   a) Tax Payer Account

b) SIDJP 9
c) SIDJP NINE
d) *Compliance Risk Management*

7. Aplikasi yang terpasang di mesin-mesin kasir dan mesin-mesin EDC untuk mendeteksi berbagai transaksi yang dilakukan oleh WP adalah…
   a) E-Biling
   b) EDC reader
   c) *Cash Receipt System*
   d) *Compliance Risk Management*

8. Berikut ini adalah yang bukan termasuk aplikasi yang masuk ke dalam kuadran *support*:
   a) *Tax Clearance*
   b) *Website & Mobile App*
   c) *Call Center*
   d) *Compliance Risk Management*

9. Tiga komponen infrastruktur TI yang perlu disediakan untuk menunjang jalannya berbagai aplikasi yang diharapkan DJP, yaitu :
   a) *Database*, Arsitektur TI, dan *Cloud*
   b) *Database, Data Recovery*, dan *Big Data*
   c) *Data Center* , Big Data, dan *Cloud*
   d) *Data Center* , *Disaster Recovery Center*, dan *Cloud*

10. Tujuan penggunaan *Cloud* yang utama adalah :
    a) Menghemat anggaran penyediaan infrastruktur
    b) Mengikuti perkembangan jaman khususnya terkait penggunaan teknologi TI
    c) memindahkan beban kepemilikan dan pengelolaan infrastruktur TI kepada penyedia layanan *Cloud*
    d) Instruksi presiden dan himbauan Menteri Komunikasi dan Informasi
    e)

6. Umpan Balik dan Tindak Lanjut

Cocokanlah jawaban anda dengan kunci jawaban Tes Formatif 1 yang terdapat di bagian akhir modul ini. Hitunglah jawaban yang benar.

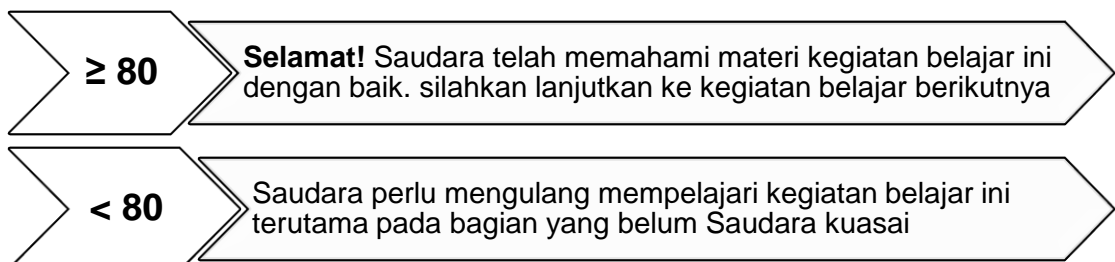
Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaaan anda terhadap materi Kegiatan Belajar 1.

$$\text{Tingkat penguasaan} = \frac{\text{Jumlah Jawaban yang Benar}}{\text{Jumlah Soal}} \times 100\ \%$$

Arti tingkat penguasaan	=	90 – 100%	= Baik Sekali
		80 – 89 %	= Baik
		70 – 79 %	= Cukup
		< 70 %	= Kurang

Penjelasan:

KEGIATAN BELAJAR

2

TATA KELOLA TIK DJP

1. Indikator

Setelah mengikuti pembelajaran, peserta diklat mampu :

- ☑ memahami latar belakang Tata Kelola TIK
- ☑ memahami Tata Kelola TIK DJP
- ☑ mempraktikkan Kebijakan Pengelolaan Keamanan Informasi
- ☑ mempraktikkan Kebijakan Pengelolaan Layanan TIK

2. Latar Belakang Tata Kelola TIK

Infrastruktur teknologi informasi pada awalnya hanya dimanfaatkan untuk mengotomasi proses-proses dan pekerjaan manual dalam suatu unit organisasi. Namun, seiring dengan semakin kompleksnya proses-proses yang harus diotomasi teknologi informasi menjadi suatu kebutuhan organisasi, tak terkecuali dengan Pemerintah.

Dunia bisnis kian berkembang, dan dukungan infrastruktur teknologi informasi pun turut berkembang dan semakin canggih, menuntut pemerintah harus mampu mengimbanginya. Mau tidak mau pemerintah harus juga mengikuti perkembangan teknologi informasi, agar tuntutan pelayanan dapat selaras dengan kebutuhan dunia bisnis.

Namun untuk mempersiapkan infrastruktur teknologi informasi ini, ternyata membutuhkan investasi yang tidak sedikit. Investasi pemerintah ini dapat bersumber dari Anggaran Pembelanjaan dan Belanja Negara (APBN), pinjaman (*loan*) ataupun dari hibah. Tentunya hal ini harus dapat dipertanggungjawabkan penggunaannya kepada seluruh rakyat, pemberi pinjaman ataupun pemberi hibah.

Di samping itu karena investasi teknologi informasi yang cukup besar tersebut, sudah tidak ekonomis lagi jika hanya ditujukan untuk meningkatkan efisiensi, efektivitas dan kecepatan kerja organisasi pemerintahan. Perkembangan teknologi informasi yang semakin canggih, harus sudah mulai diarahkan menjadi *enabler* terhadap peningkatan kinerja suatu organisasi.

Dan tentunya tanggung jawab pengelolaan teknologi informasi tidak bisa sepenuhnya diserahkan ke unit yang hanya khusus menangani teknologi informasi secara teknikal sebagaimana pendekatan manajemen konvensional, melainkan juga harus menjadi tanggung jawab berbagai pihak manajemen dalam suatu organisasi.

Hal inilah yang kemudian melahirkan konsep dan paradigma baru dalam mengelola Teknologi Informasi yang disebut dengan *Tata Kelola Teknologi Informasi (IT Governance).*

Apa itu Tata Kelola TI (*IT Governence)?*

Banyak definisi mengenai Tata Kelola TI yang telah dikembangkan oleh para ahli dan peneliti, diantaranya :

IT Governance Institute, 2003 dalam Putra,et.al.(2008), mendefinisikan Tata Kelola TI sebagai berikut :

> *"IT Governance is the responsibility of the board of directors and executive management. It is an integral part of Enterprise Governance and consists of the leadeship and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives".*

Weill & Ross (2004) dalam Putra et.al (2008). memberikan pendefinisian tata kelola TI sebagai berikut:

> *"IT Governance is defined as specifying the decision rights and accountability model to encourage desirable behavior in IT usage".*

Berdasarkan penelitian *ICT Governance* yang dikembangkan Australia yaitu AS8015 (2005), dalam Putra et.al. (2008), mendefinisikan tata kelola TI*:*

> *"The system by which the current and future use of ICT is directed and kontrolled. It involves evaluating and directing the plans for the use of ICT to support the organisation and monitoring this use to achieve plans. It includes the strategy and policies for using ICT within an organisation".*

Oltsik dalam Grewal, et,al. (2005), mendefinisikan IT Governance sebagai *“as a set of policies, processes, and procedures that support everything that IT does”.*

Walaupun definisi yang para ahli berbeda pada beberapa aspek, namun mereka fokus pada isu yang sama yaitu bagaimana TI dapat memberikan *value* dengan menyelaraskan hubungan antara TI dan proses bisnis serta bagaimana dengan TI dapat mengurangi atau mengendalikan risiko.

Teknologi informasi Komunikasi (TIK) yang sangat berkembang sudah menjadi kebutuhan yang sangat penting bagi hampir semua organisasi karena dipercaya dapat membantu meningkatkan efektifitas dan efisiensi proses bisnis organisasi, tak terkecuali Direktorat Jenderal Pajak (DJP). Untuk mencapai hal tersebut diperlukan suatu pengelolaan TIK yang baik dan benar agar keberadaan TI mampu untuk menunjang kesuksesan DJP dalam pencapaian tujuannya. Bahkan saat ini kesuksesan tata kelola organisasi mempunyai ketergantungan terhadap sejauh mana tata kelola TI (*IT Governance*) dilakukan.

Dalam menjalankan tugas dan fungsinya, Direktorat Jenderal Pajak (DJP) memberdayakan dan mengandalkan infrastruktur TIK yang pengadaannya membutuhkan pertanggungjawaban terkait penggunaan anggaran publik.

Bentuk tanggung jawab yang dibutuhkan diantaranya adalah adanya jalur kepemimpinan yang jelas dan transparan dalam penyelenggaraan TIK dan harus mencakup keseluruhan aspek mulai dari perencanaan, pengadaan, implementasi, penyediaan layanan, pengamanan aset informasi, kelangsungan layanan, dan evaluasinya.

Keseluruhan aspek tersebut harus dikelola melalui suatu kerangka kerja yang baku yang menjadi dasar penyusunan maupun penerapan kebijakan teknis terkait TIK, dan yang wajib dipatuhi oleh setiap unit kerja di DJP. Untuk mengakomodasi kebutuhan tersebut, maka disusun kerangka kerja kebijakan Tata Kelola TIK DJP.

3. Kebijakan Tata Kelola TIK DJP

Tata Kelola TIK DJP adalah suatu kerangka kerja yang mengatur dan mengelola keseluruhan proses perencanaan, realisasi, operasional harian, pengamanan, kelangsungan layanan, dan evaluasi internal penyelengaraan TIK DJP melalui jalur kepemimpinan yang tegas dan transparan.

Tata Kelola TIK DJP ini disusun dengan format penyusunan yang dibagi berdasarkan fungsi, dengan struktur wilayah pembagian sebagai berikut:

a. Tata Kelola Teknologi Informasi dan Komunikasi, yang merupakan kebijakan umum tentang keseluruhan aspek Tata Kelola TIK di Direktorat Jenderal Pajak dan merupakan kerangka kerja utama dalam pengelolaan TIK;
b. Pengelolaan Keamanan Informasi, yang merupakan kebijakan pengelolaan keamanan informasi baik di lingkungan Direktorat Jenderal Pajak maupun mitra- kerjanya;
c. Pengelolaan Layanan Teknologi Informasi dan Komunikasi, yang merupakan kebijakan pengaturan pengelolaan berbagai bentuk layanan TIK di Direktorat Jenderal Pajak;
d. Pengembangan TIK, yang merupakan kebijakan pengaturan pengembangan TIK, baik secara internal maupun yang dilakukan oleh pihak mitra kerja DJP;
e. Pengelolaan Proyek TIK, yang merupakan kebijakan pengelolaan proyek TIK di lingkungan Direktorat Jenderal Pajak;
f. Pengelolaan Kelangsungan Layanan Teknologi Informasi dan Komunikasi, yang merupakan kebijakan pengelolaan kegiatan yang bertujuan untuk menjaga kelangsungan layanan TIK Direktorat Jenderal Pajak;
g. Pemantauan dan Evaluasi Kinerja Teknologi Informasi dan Komunikasi, yang merupakan kebijakan pemantauan dan evaluasi kinerja TIK sebagai bagian dari sinergi TIK dalam pencapaian target Tugas Pokok dan Fungsi Direktorat Jenderal Pajak.

Selanjutnya kebijakan tersebut dijabarkan ke dalam 7 (tujuh) buku yang berisi 7 (tujuh) kerangka kerja kebijakan dalam pelaksanaan Tata Kelola TIK DJP, yaitu:

a. Buku Satu tentang Kebijakan Tata Kelola TIK DJP berisi kebijakan umum yang mengatur kerangka kerja pengelolaan TIK, Tim Pengarah Tata Kelola TIK DJP, dan *Chief Information Officer (CIO)* DJP;
b. Buku Dua tentang Kebijakan Pengelolaan Keamanan Informasi berisi prinsip dasar dalam upaya melindungi kerahasiaan, keutuhan, dan ketersediaan aset informasi DJP dari segala bentuk gangguan dan ancaman baik yang berasal dari dalam maupun dari luar DJP, baik yang dilakukan secara sengaja maupun tidak sengaja;

c. Buku Tiga tentang Kebijakan Pengelolaan Layanan TIK berisi prinsip dasar pengelolaan layanan TIK yang berkualitas di DJP;
d. Buku Empat tentang Kebijakan Pengembangan TIK berisi prinsip dasar pengembangan TIK yang berkualitas di DJP, yang bertujuan untuk memberi panduan bagi pengguna layanan TIK mengenai tata cara untuk melakukan interaksi dengan unit kerja TIK DJP dalam pengembangan TIK, mengurangi tingkat kesalahan pada pengembangan TIK, dan mengurangi pekerjaan ulang yang harus dilakukan karena adanya kesalahan pengembangan;
e. Buku Lima tentang Kebijakan Pengelolaan Proyek berisi prinsip dasar pengelolaan proyek TIK di lingkungan DJP agar dapat diselesaikan tepat waktu dan memberikan hasil sesuai dengan yang direncanakan, serta menjamin penerapan metodologi pengelolaan proyek secara konsisten terhadap seluruh proyek TIK di DJP;
f. Buku Enam tentang Kebijakan Pengelolaan Kelangsungan Layanan TIK berisi prinsip dasar penyelenggaraan kelangsungan proses bisnis inti atau kritikal di DJP yang memerlukan dukungan layanan TIK dan tersedianya prosedur serta perangkat pemulihan layanan TIK pada keadaan darurat secara cepat, tepat biaya, dan dengan risiko yang terkendali; dan
g. Buku Tujuh tentang Kebijakan Pemantauan dan Evaluasi Kinerja TIK berisi prinsip dasar pengelolaan kegiatan pemantauan dan evaluasi kinerja TIK untuk menjamin metodologi pemantauan dan evaluasi kinerja TIK dilaksanakan secara konsisten.

Kebijakan Tata Kelola TIK yang diatur melalui PER-37/PJ/2010 atau yang disebut Buku Satu ini merupakan payung hukum dari enam kebijakan lainnya.

Kebijakan dalam Buku Satu ini merupakan kebijakan umum yang harus dijadikan pegangan dalam pengelolaan TIK. Di samping itu buku ini secara khusus mengatur tanggung jawab dari Tim Pengarah Tata Kelola TIK DJP dan *CIO* DJP. Hal ini dikarenakan bahwa Tim Pengarah Tata Kelola TIK DJP merupakan unsur yang memastikan bahwa kebijakan umum dilaksanakan dengan baik oleh pihak-pihak terkait

Tim Pengarah Tata Kelola TIK DJP adalah tim yang dibentuk oleh Direktur Jenderal Pajak untuk mengarahkan penyelenggaraan Tata Kelola TIK agar sesuai dengan Rencana Strategis DJP. Dan *Chief Information Officer (CIO)* DJP adalah seorang Pejabat Eselon II unit kerja TIK yang ditunjuk oleh Direktur Jenderal

Pajak untuk mengoordinasikan seluruh pelaksanaan kerangka kerja Tata Kelola TIK DJP.

Kebijakan Tata Kelola TIK DJP ini dibentuk dengan mengacu kepada perangkat hukum yang berlaku, standar industri, dan keperluan internal di DJP. Standar industri yang digunakan sebagai acuan adalah:

a. COBIT (*Control Objective for Information and Related Technology*) 4.1 dari *IT Governance Institute*, Amerika Serikat, untuk aspek Perencanaan (*Plan*) dan Pengorganisasian (*Organise*); pengembangan (*Acquire*) dan implementasi (*Implement*); pelayanan (*Deliver*) dan perawatan (*Support*); serta pemantauan (*Monitor*) dan evaluasi (*Evaluate*)
b. ITIL (Information Technology Infrastructure Library) V2 dari Office of Government Commerce, Britania Raya;
c. ISO/IEC 38500 (*Corporate governance of information technology*) dari Badan Standar Internasional ISO;
d. ISO/IEC 20000 (*Information technology - Service management*) dari Badan Standar Internasional ISO;
e. ISO/IEC 27001 (Information technology – Security techniques – Information security management system – Requirements)dari Badan Standar Internasional ISO;
f. ISO/IEC 27002 (Information technology – Security techniques – Code of Practice for information security management)dari Badan Standar Internasional ISO;
g. ISO/IEC 24762 (Information technology – Security techniques – Guidelines for information and communications technology disaster recovery services) dari Badan Standar Internasional ISO;
h. ISO/IEC 27005 (BS7799-3:2006) (*Risk Management System)* dari Badan Standar Internasional ISO;
i. BS (British Standard) 25999 (Business Continuity Management);
j. PMBOK (Project Management Body of Knowledge) 2007 dari Project Management Institute, Amerika Serikat; dan
k. CMMI (Capability Maturity Model Integration) dari *Software Engineering Institute*, Amerika Serikat.

Tata Kelola Teknologi Informasi dan Komunikasi (TIK) diterapkan di DJP dalam rangka untuk:

a. Mengelola penggunaan TIK sesuai standar mutu yang jelas, sehingga dalam menjalankan tugas dan fungsinya, khususnya dalam menyelenggarakan layanan perpajakan dapat dilaksanakan secara efektif, efisien, dan aman;
b. Menyelaraskan kesesuaian investasi, pembelanjaan, dan pengadaan TIK dengan rencana kegiatan maupun tugas DJP;
c. Memastikan kedisiplinan serta menjaga standar mutu identifikasi dan penyusunan perencanaan strategis TIK untuk jangka pendek dan jangka panjang;
d. Memastikan tercapainya standar pengkajian kelayakan dan kesesuaian prioritas pelaksanaan kegiatan proyek dan pengadaan TIK dengan misi dan tugas DJP;
e. Memastikan bahwa inisiatif terkait penerapan TIK dikomunikasikan kepada semua pihak terkait, baik di dalam lingkungan DJP, pejabat pimpinan Kementerian Keuangan, maupun mitra kerjanya;
f. Memastikan tercapainya standar mutu koordinasi dan pemantauan penerapan inisiatif TIK, pengkajian ulang maupun evaluasi kinerja kegiatan penerapan infrastruktur TIK, pengamanan keseluruhan aset informasi DJP, dan penyelenggaraan layanan TIK;
g. Meningkatkan kinerja dan mutu pengelolaan TIK khususnya dalam menyelenggarakan layanan perpajakan;
h. Tersedianya kerangka kerja pemantauan pelaksanaan seluruh kegiatan TIK dan pengarahannya agar sasaran kinerja TIK yang telah ditetapkan dapat tercapai;
i. Memastikan bahwa kerangka kerja pengelolaan TIK didukung oleh kelengkapan kerangka kerja kebijakan dan prosedur teknis yang dibutuhkan, serta dapat diberlakukan secara efektif di semua unit kerja DJP; dan
j. Memastikan kelangsungan layanan TIK bagi kepentingan layanan proses perpajakan di DJP.

Dalam penyelenggaraan Tata Kelola TIK, aspek pengelolaan risiko digunakan agar layanan TIK dan pengamanan aset informasi dapat terselenggara dengan baik. Semua inisiatif yang berkaitan dengan TIK di DJP harus tidak bertentangan serta sejalan dengan perundang-undangan maupun kerangka kerja hukum lainnya yang berlaku.

4. Kebijakan Pengelolaan Keamanan Informasi

Kebijakan Pengelolaan Keamanan Informasi adalah kerangka kerja manajemen pengamanan aset informasi yang menggunakan pendekatan berbasis risiko dalam menyusun, menerapkan, melaksanakan, mengawasi, mengkaji, memelihara, dan meningkatkan kinerja pengelolaan keamanan informasi.

Kebijakan Pengelolaan Keamanan Informasi DJP disusun dengan tujuan untuk:

a. Mendukung DJP dalam mencapai salah satu sasarannya yaitu melaksanakan modernisasi di bidang teknologi informasi dan komunikasi;
b. Menyediakan perangkat pengaturan dalam pengelolaan keamanan informasi; dan
c. Melindungi kerahasiaan, keutuhan, dan ketersediaan aset informasi DJP dari segala bentuk gangguan dan ancaman baik dari dalam maupun luar DJP, yang dilakukan secara sengaja atau tidak.

Area yang diatur dalam Buku Dua terkait Kebijakan Pengelolaan Keamanan Informasi meliputi:

a. Pengelolaan Aset Informasi;
b. Pengaturan Keamanan Informasi Pihak Ketiga;
c. Pengaturan Keamanan Informasi Sumber Daya Manusia;
d. Keamanan Fisik dan Lingkungan;
e. Pengelolaan Komunikasi dan Operasional;
f. Pengendalian Akses ke Aset Informasi;
g. Keamanan Informasi dalam Pengembangan dan Pemeliharaan Sistem Informasi;
h. Pengelolaan Gangguan Keamanan Informasi;
i. Keamanan Informasi dalam Pengelolaan Kelangsungan Layanan TIK; dan
j. Kepatuhan

4.1. Pengelolaan Aset Informasi

Kebijakan Pengelolaan Aset Informasi ini bertujuan untuk memberi acuan dalam mengelola perlindungan keamanan yang memadai akan aset informasi DJP

dan memastikan bahwa aset informasi memiliki tingkat perlindungan keamanan yang sesuai dengan klasifikasinya.

Aset informasi diklasifikasikan menjadi 4 (empat) golongan sebagai berikut:

a. **Sangat rahasia** yaitu aset informasi yang bersifat strategis bagi DJP dan berisiko sangat tinggi yang pembocoran atau akses tanpa izin terhadapnya mempunyai konsekuensi hukum. Informasi ini hanya dapat diakses secara sangat terbatas oleh pihak ketiga dan hanya dapat digunakan untuk kepentingan atau karena kewajiban dan kebutuhan DJP, dengan syarat pihak ketiga dan pegawai pihak ketiga menandatangani Kesepakatan Kewajiban Menjaga Rahasia/*Non-Disclosure Agreement* (NDA).

   Contoh aset informasi sangat rahasia: Data Wajib Pajak.

b. **Rahasia** yaitu aset informasi yang sangat peka dan berisiko tinggi atau yang menurut peraturan perundang-undangan dinyatakan rahasia yang pembocoran atau penyalahgunaan akses terhadapnya dapat mengganggu kelancaran kegiatan DJP atau mengganggu citra dan reputasi DJP. Informasi ini hanya dapat diakses secara terbatas oleh pihak ketiga dan hanya dapat digunakan untuk kepentingan atau karena kewajiban dan kebutuhan DJP melalui serah terima resmi dengan syarat pihak ketiga dan pegawai pihak ketiga menandatangani Kesepakatan Kewajiban Menjaga Rahasia/*Non-Disclosure Agreement*.

   Contoh aset informasi rahasia: *IP address*, *password* komputer, bahan/ materi pelatihan, rencana anggaran/pengadaan, data gaji dan penilaian kinerja pegawai, serta data kesehatan pribadi pegawai yang secara legal harus dilindungi.

c. **Terbatas** yaitu aset informasi yang telah terdistribusi secara luas di lingkungan internal DJP yang penyebarannya secara internal tidak lagi memerlukan izin dari Pemilik Aset Informasi dan risiko penyebarannya oleh pihak yang tidak berwenang tidak menimbulkan kerugian yang berarti. Informasi ini dapat diberikan kepada pihak ketiga oleh pemiliknya untuk kepentingan dinas melalui prosedur serah terima resmi.

Contoh aset informasi terbatas: kebijakan DJP, panduan kerja, tata cara kerja, instruksi kerja, memo/publikasi internal, informasi yang disediakan dalam intranet, dan data operasional IT lainnya.

d. **Publik** yaitu aset informasi yang secara sengaja disediakan oleh DJP untuk dapat diketahui masyarakat umum.

   Contoh aset informasi publik: brosur, situs publik DJP, dan siaran pers (*press release*).

Kebijakan Pengelolaan Aset Informasi ini mencakup hal-hal sebagai berikut:

a. Pengelolaan daftar inventaris dan aturan penggunaan aset informasi;
b. Pengklasifikasian aset informasi;
c. Pemberian label pada aset informasi;
d. Pedoman Pengelolaan Aset Informasi.

Kebijakan dan aturan penggunaan aset-aset informasi ditetapkan dan berlaku bagi seluruh pegawai dan pihak ketiga. Seluruh pengguna aset informasi tanpa kecuali harus mematuhi kebijakan dan aturan yang telah ditetapkan dan harus melaporkan kepada penanggung jawab keamanan informasi terkait apabila melihat terjadinya pelanggaran terhadap kebijakan ini.

4.2. Pengaturan Keamanan Informasi Pihak Ketiga

Kebijakan Pengaturan Keamanan Informasi Pihak Ketiga ini bertujuan untuk memberi acuan dalam memelihara keamanan aset informasi dan perangkat pengolah informasi yang diakses, diproses, dikomunikasikan, atau dikelola pihak ketiga.

Yang dimaksud dengan pihak ketiga adalah pihak penyedia barang/jasa yang menjadi mitra DJP, kementerian/instansi lain terkait, dan pihak ketiga lainnya.

Kebijakan Pengaturan Keamanan Informasi Pihak Ketiga ini mencakup hal-hal sebagai berikut:

a. Identifikasi, evaluasi, dan pengendalian risiko melalui perjanjian kontrak dengan pihak ketiga;
b. Perjanjian kontrak antara pihak ketiga dengan tenaga kerja/pegawai yang digunakan untuk menyediakan layanan dan/atau melakukan pekerjaan di DJP;
c. Pedoman Akses Pihak Ketiga.

Akses terhadap aset informasi di lingkungan DJP hanya boleh diberikan dalam rangka pelaksanaan tugas/kegiatan DJP serta harus dikontrol secara ketat. Sebelum memberikan akses kepada pihak ketiga, pegawai DJP yang berwenang memberikan akses harus mendeteksi dan mengevaluasi risiko-risiko yang mungkin muncul sehubungan dengan pemberian akses serta harus menerapkan kontrol yang memadai untuk mengurangi dampak atau mencegah terjadinya risiko-risiko tersebut.

Evaluasi risiko dilakukan dengan memperhatikan aspek-aspek sebagai berikut:

a. Jenis akses yang diperlukan : Akses fisik ke kantor, ruang kerja, atau ruang *server*; dan Akses non-fisik ke dalam jaringan, basis data, dan sistem informasi;
b. Alasan kebutuhan akses:
    1) Operasional dan dukungan (*support*) pada perangkat keras dan perangkat lunak;
    2) Audit keamanan informasi; dan
    3) Pengembangan aplikasi dan sistem informasi.
c. Metode akses, misalnya akses melalui jaringan lokal, akses melalui modem (*dial in*), atau akses melalui fasilitas VPN IP - jaringan komunikasi pribadi (biasanya digunakan dalam suatu organisasi atau oleh beberapa entitas yang berbeda) untuk berkomunikasi melalui jaringan publik, dalam hal ini menggunakan *internet protocol*.

Pengendalian risiko pemberian akses pada pihak ketiga dilakukan antara lain melalui klausul-klausul dalam perjanjian kontrak dan melalui perjanjian Kesepakatan Kewajiban Menjaga Rahasia (*Non-Disclosure Agreement/NDA*). Pemberian akses tersebut hanya boleh diberikan setelah penandatanganan NDA.

4.3. Pengelolaan Keamanan Informasi Sumber Daya Manusia

Kebijakan Pengelolaan Keamanan Informasi Sumber Daya Manusia ini bertujuan untuk memberi acuan dalam:

a. Memastikan bahwa pegawai dan pihak ketiga memahami tanggung jawabnya yang sesuai dengan peran terkait penugasannya, dan untuk

mengurangi risiko pencurian, penyalahgunaan dan kesalahan pemanfaatan aset informasi.

b. Memastikan bahwa pegawai dan pihak ketiga mengetahui ancaman maupun hal- hal yang utama dari keamanan, tanggung jawab dan perannya, serta telah dibekali pelatihan untuk mendukung kebijakan keamanan DJP dan mengurangi kesalahan dalam pekerjaannya.
c. Memastikan bahwa pegawai dan pihak ketiga menjalani prosedur terkait keamanan informasi sebelum, selama, dan saat akan mengakhiri tugas di DJP.

Kebijakan Pengelolaan Keamanan Informasi Sumber Daya Manusia ini mencakup pengelolaan keamanan informasi terhadap pegawai dan pihak ketiga yang diterapkan sebelum bertugas, selama bertugas, dan saat akan mengakhiri tugas dan pekerjaan di DJP.

Setiap Pejabat Keamanan Informasi harus menyusun daftar pegawai dengan keahlian khusus atau yang berada di posisi kunci di unit kerjanya yang perlu mendapat perhatian khusus pada saat pegawai yang bersangkutan akan mengalami penghentian atau mutasi.

Pegawai dengan keahlian khusus atau yang berada di posisi kunci berkewajiban untuk melakukan alih keahlian dan pengetahuan kepada rekan kerjanya agar sebelum meninggalkan atau keluar dari unit kerjanya, pekerjaan yang menjadi tugasnya dapat terjamin keberlangsungannya.

Pegawai dan pihak ketiga yang akan berhenti bekerja atau habis masa kontrak kerjanya dengan DJP harus mengembalikan seluruh aset yang dipergunakan selama bekerja di DJP kepada pemilik aset informasi.

Pejabat Keamanan Informasi berhak untuk menghentikan/menutup untuk sementara atau selamanya hak menggunakan aset informasi bagi pegawai yang sedang menjalani pemeriksaan yang terkait dengan dugaan adanya pelanggaran terhadap Kebijakan Pengelolaan Keamanan Informasi dan/atau bagi pegawai yang sedang menjalani proses hukum.

Hak akses terhadap sistem informasi yang dimiliki pegawai akan dicabut secara otomatis bila pegawai yang bersangkutan dimutasikan ke unit kerja lain di lingkungan DJP atau tidak lagi bekerja di DJP. Begitupun dengan hak akses terhadap sistem informasi yang dimiliki pihak ketiga akan dicabut secara otomatis bila yang bersangkutan tidak lagi bekerja di lingkungan DJP.

4.4. Keamanan Fisik Dan Lingkungan

Kebijakan Keamanan Fisik dan Lingkungan ini bertujuan untuk memberi acuan dalam mencegah akses fisik yang tidak terotorisasi, kerusakan, dan intervensi kepada perangkat dan informasi DJP serta mencegah kehilangan, kerusakan, pencurian atau kejadian yang membahayakan aset informasi dan mengganggu akitivitas DJP.

Kebijakan Keamanan Fisik dan Lingkungan ini mencakup hal-hal sebagai berikut:

a. Pengamanan lingkungan kerja dan *Data Center*;
b. Pengamanan perangkat/peralatan pengolah informasi;
c. Pedoman Pengamanan Perangkat dan Fasilitas Pengolahan Data dan Informasi.

Kebijakan yang diterapkan untuk mengamankan lingkungan kerja maupun *Data Center*, diantaranya :

a. Ruangan khusus (*Data Center*/DC dan ruang *server*) dilindungi dengan pengamanan fisik yang memadai dan berfungsi dengan baik seperti pintu elektronik, sistem pemadam kebakaran, alarm bahaya, dan perangkat pemutus aliran listrik harus tersedia untuk menyimpan *server*, infrastruktur jaringan dan komunikasi data, serta fasilitas pengolah dan pengelola informasi sensitif lainnya;
b. Ruangan *Data Center* memiliki area sesuai aktivitas yang dapat dilakukan dalam area tersebut. Setiap area memiliki identifikasi dan tingkat kewenangan/otorisasi yang diperlukan bagi pengguna yang akan mengakses *Data Center sebagai berikut*:

1) Area *Staging:* area untuk membuka kemasan *hardware* dan *pre-installed software* sebelum dipindahkan ke *area server*;
2) Area Operator: area yang dilengkapi *console* untuk akses *server* secara *remote* tanpa harus memasuki area *server*;
3) Area *Server:* area *Data Center* utama dan hanya petugas yang berwenang saja yang dapat mengakses area ini;
    a. Area *Library:* area untuk menyimpan media *backup*; dan
4) Area *Network*: area untuk menyimpan perangkat-perangkat utama jaringan.

c. Akses keluar masuk ruangan *Data Center* dan area kerja lainnya yang berisikan aset informasi yang bersifat rahasia dan sangat rahasia harus dibatasi dan hanya diberikan kepada pegawai tertentu yang berwenang;
d. Seluruh pegawai, pihak ketiga, atau tamu yang memasuki ruangan *Data Center* atau area kerja yang berisikan aset informasi yang bersifat rahasia dan sangat rahasia harus didampingi oleh pegawai DJP tertentu yang berwenang. Waktu masuk dan keluar serta maksud kedatangannya harus dicatat dalam buku catatan keluar masuk ruangan (*log book*);
e. Kantor, ruangan, dan fasilitas yang berisikan informasi rahasia dan sangat rahasia harus memiliki pengamanan fisik yang memadai. Sebagai contoh, pintu dan jendelanya harus dikunci jika ditinggalkan;
f. Pengambilan gambar di ruangan *Data Center* dan ruang *server* harus dengan seijin penanggung jawab ruang tersebut; dan
g. Ruang s*erver*, *Data Center*, dan *Disaster Recovery Center* (DRC) tidak boleh digunakan untuk ruang kerja.

Untuk mengamankan peralatan/perangkat pengolah informasi, kebijakan yang diterapkan adalah sebagai berikut:

a. Perangkat pengolah informasi harus ditempatkan di lokasi yang tidak dilewati/dilalui oleh tamu atau pihak ketiga;
b. Perangkat pengolah informasi termasuk mesin faksimili, *printer*, atau komputer yang digunakan untuk memproses informasi rahasia dan sangat rahasia harus ditempatkan di lokasi yang aman untuk mencegah kebocoran informasi tersebut ke pihak yang tidak berwenang;
c. Makanan dan minuman dilarang untuk dibawa masuk ke atau dikonsumsi di dalam ruang *server* dan *Data Center*. Semua area yang digunakan untuk menyimpan aset informasi penting adalah area bebas rokok;
d. Area yang digunakan untuk menyimpan aset informasi penting seperti ruang arsip, ruang *server, Data Center*, *Disaster Recovery Center,* ruang alat komunikasi, atau ruang penyimpanan media harus mendapatkan perlindungan yang layak dari dampak lingkungan/polusi dengan aliran udara (ventilasi), suhu, dan kelembaban yang sesuai;
e. Batas minimum dan maksimum untuk suhu dan kelembaban di dalam ruang *server, Data Center, dan Disaster Recovery Center* harus ditetapkan

mengikuti standar yang disyaratkan oleh pabrikan perangkat dan harus selalu dilakukan pengawasan. Tindakan untuk mengembalikan kondisi suhu dan kelembaban sesuai batasan harus segera diterapkan apabila terjadi kondisi yang menyebabkan dilanggarnya standar tersebut;

f. Sistem perlindungan kebakaran harus dipasang dengan aman agar tidak membahayakan personel yang bekerja di ruang *server, Data Center*, dan *Disaster Recovery Center*, dan harus dirawat secara teratur untuk melindungi fasilitas dan perangkat yang ada di dalamnya;

g. Fasilitas untuk melindungi perangkat pengolah informasi dari sambaran petir harus dipasang di semua unit kerja DJP;

h. Semua perangkat pengolah informasi harus mendapatkan pasokan daya yang sesuai dengan spesifikasi yang disyaratkan oleh pabrikan perangkat. Untuk setiap lokasi kerja termasuk ruang *server, Data Center, dan Disaster Recovery Center harus* tersedia pasokan listrik yang cukup untuk beban maksimal seluruh perangkat, termasuk perangkat pendukung yang ada di lokasi tersebut;

i. Pasokan listrik yang digunakan untuk mengoperasikan perangkat pengolah informasi di DJP harus mempunyai sumber alternatif dengan daya dan jangka waktu ketersediaan atau jangka waktu pengoperasian yang cukup. Pasokan ini paling sedikit harus berupa perangkat generator listrik dan perangkat UPS (*Uninterruptable Power Supply*) dengan daya yang cukup dan dengan konfigurasi yang dapat memindahkan pasokan listrik tanpa gangguan terhadap perangkat komputer/*server*;

j. Instalasi jaringan listrik harus disesuaikan dengan standar keselamatan yang ada;

k. Harus tersedia koneksi ke penyedia layanan telekomunikasi alternatif dengan jalur kabel data yang berbeda;

l. Konfigurasi jaringan kabel data dan daya harus terekam dalam dokumen resmi yang dimutakhirkan untuk setiap perubahan;

m. Jaringan kabel data harus dipisahkan dari jaringan kabel listrik dengan jarak yang cukup untuk menghindari dampak radiasi (elektromagnet), dan dengan pencantuman label yang sesuai;

n. Jaringan kabel data atau koneksi yang menghubungkan perangkat komputer/*server* yang penting harus diamankan melalui:

1) Konstruksi jalur kabel data yang dapat melindungi kabel dari dampak lingkungan atau pihak yang tidak berwenang;
2) Spesifikasi kabel data yang sesuai dengan ancaman lingkungan (air, suhu/panas, kotoran, atau radiasi);
3) Proses inspeksi dan perawatan rutin; dan
4) Penempatan yang terlindung dari ancaman sekitar (jalur lintas kendaraan, peralatan berat, atau pekerjaan konstruksi);

o. Seluruh perangkat pengolah informasi penting dan peralatan pendukung harus diperiksa dan diujicoba efektivitasnya secara teratur/berkala, dirawat, dan dibersihkan sesuai dengan spesifikasi pabrikannya;

p. Perawatan dan perbaikan perangkat pengolah informasi hanya dapat dilakukan oleh pegawai yang berwenang dan mempunyai kompetensi teknis yang sesuai.

4.5. **Pengelolaan Komunikasi Dan Operasional**

Kebijakan Pengelolaan Komunikasi dan Operasional ini bertujuan untuk memberi acuan dalam:

a. Memastikan operasional dari fasilitas pengolah informasi yang tepat dan aman.
b. Melindungi integritas dari perangkat lunak dan informasi.
c. Memelihara integritas dan ketersediaan dari informasi dan fasilitas pengolah informasi.
d. Memastikan perlindungan informasi yang melalui jaringan beserta infrastruktur pendukungnya.
e. Mencegah tindakan pengungkapan, perubahan, pemindahan atau penghancuran aset informasi yang tidak terotorisasi, dan gangguan pada aktivitas/pekerjaan DJP.
f. Memelihara keamanan dari informasi dan perangkat lunak yang dipertukarkan baik diinternal DJP maupun dengan pihak luar.
g. Mendeteksi aktivitas pengolahan/penggunaan informasi yang tidak terotorisasi.

Kebijakan Pengelolaan Komunikasi dan Operasional ini mencakup hal-hal sebagai berikut:

a. Kelancaran operasional dalam pengelolaan keamanan informasi;
b. Kontrol-kontrol untuk mendeteksi dan mencegah masuknya perangkat lunak yang membahayakan ke dalam jaringan komputer DJP;
c. Backup dan Restore;
d. Perlindungan keamanan jaringan;
e. Penanganan media penyimpanan informasi;
f. Pengamanan pertukaran informasi;
g. Pemantauan pelaksanaan pengelolaan keamanan informasi;
h. Pedoman Backup dan Restore Sistem/Data/Informasi;
i. Pedoman Enkripsi dan *Key Management;*
j. Pedoman Penggunaan *User Account*/*Password* dan Pengamanan *Log-on* ke dalam Fasilitas Teknologi Informasi, Penggunaan Fasilitas *e-Mail*, serta
k. Penggunaan Akses Internet dan Intranet.

Untuk menjamin kelancaran operasional dalam hal pengelolaan keamanan informasi, maka kebijakan yang diterapkan adalah sebagai berikut:

a. Seluruh prosedur operasional yang terkait dengan penggunaan perangkat pengolah informasi dan komunikasi didokumentasikan, dirawat, dan dapat diperoleh dengan mudah oleh pegawai yang membutuhkannya.
b. Perubahan terhadap perangkat lunak maupun fasilitas pengolah dan pengelola informasi harus dikontrol dan mengacu kepada Kebijakan Pengelolaan Layanan TIK.
c. Harus dilakukan pemisahan tugas pegawai pada proses-proses yang berbasis komputer yang melibatkan informasi rahasia atau sangat rahasia, berharga, dan rawan, agar tidak ada pegawai yang memiliki kontrol menyeluruh terhadap semua aset informasi.
d. Untuk mengurangi peluang modifikasi aset informasi oleh pihak yang tidak berwenang atau peluang terjadinya kesalahan dalam penggunaan sistem informasi, harus dijamin adanya pemisahan antara fasilitas pengembangan, pengujian, dan operasional.
e. Untuk menghindari penyalahgunaan akses atau terjadinya perubahan sistem yang tidak dikehendaki, pengembangan dan pengujian perangkat

lunak harus dilakukan pada perangkat yang berbeda dari yang digunakan untuk operasional.

f. Alat bantu pengembangan seperti *compiler* atau *editor* dan alat bantu sistem (*system utilities)* tidak boleh diakses dari sistem operasional kecuali apabila diperlukan.
g. Jika pengelolaan atas fasilitas pengolah informasi diserahkan kepada mitra kerja/pihak ketiga, maka Ketua Tim Keamanan Informasi DJP harus memastikan dilakukannya evaluasi terhadap risiko dan ditetapkannya kontrol-kontrol untuk mengurangi setiap potensi kerusakan atau kehilangan data. Kontrol-kontrol ini harus disertakan dalam kontrak kerja yang dibuat dengan mitra kerja/pihak ketiga tersebut.

Kontrol-kontrol yang diterapkan untuk mendeteksi dan mencegah masuknya perangkat lunak yang membahayakan ke dalam jaringan komputer DJP meliputi:

a. Penggunaan perangkat lunak berlisensi;
b. Pemasangan perangkat lunak anti-*virus*; dan
c. Kewajiban pengguna (*user*) untuk memeriksa lampiran (*attachment*) surat elektronik (*e-mail*) dan arsip (*file*) yang diambil dari Internet dari kandungan *virus/trojan/malware* sebelum digunakan.

Untuk menjamin keamanan informasi dalam hal *backup* dan r*estore*, maka kebijakan yang diterapkan adalah sebagai berikut:

a. Seluruh informasi penting dan rawan yang dikelola DJP harus di-*backup* secara berkala untuk menjamin keutuhan dan ketersediaannya pada saat diperlukan.
b. Informasi yang rahasia dan sangat rahasia harus disimpan di server dengan akses terbatas.
c. Penyimpanan informasi rahasia dan sangat rahasia di komputer atau tempat penyimpanan data lokal (*local storage*) harus disetujui oleh pejabat yang berwenang;
d. Data yang disimpan di server harus di-*backup* sesuai dengan prosedur *backup,* dan seluruh *backup* harus disimpan secara aman;
e. Masa retensi penyimpanan media *backup* dan jenis *backup* terhadap data maupun sistem tertentu akan ditentukan kemudian oleh Tim Keamanan Informasi sesuai dengan jenis data/ sistem yang di-*backup*; dan

f. Apabila terdapat kegagalan sistem yang membutuhkan proses *restore*, maka harus dipastikan bahwa *baseline* yang dipakai tersedia dalam media *backup.*

Dalam rangka melindungi keamanan jaringan, kebijakan yang diterapkan adalah sebagai berikut:

a. Jaringan harus dilindungi dari akses oleh pihak yang tidak berwenang dengan menerapkan kontrol-kontrol yang tepat.
b. Kegiatan jaringan akan dipantau untuk menjamin bahwa sumber daya jaringan digunakan secara efektif dan efisien dan agar tidak terjadi kesalahan dalam pemrosesan jaringan;
c. Penyambungan atau perluasan jaringan komputer dan akses ke sistem jaringan internal atau eksternal ditentukan berdasarkan kebutuhan kegiatan DJP dan dikendalikan serta diatur oleh unit kerja TIK DJP;
d. Wewenang pengguna untuk memasuki jaringan komputer harus dibatasi sesuai dengan layanan yang secara resmi telah ditetapkan;
e. Setiap sistem yang mengandung aplikasi penting yang dikelola DJP atau yang memberi akses ke informasi yang rahasia dan sangat rahasia harus dipasangi perangkat *firewall* untuk melindungi aplikasi dan informasi tersebut dari akses oleh pihak yang tidak berwenang;
f. Akses ke internet diijinkan dalam rangka mendukung pelaksanaan kegiatan DJP, serta untuk meningkatkan kompetensi dan pengetahuan pegawai DJP;
g. Akses ke internet harus menggunakan perangkat lunak yang aman dan melalui *gateway* internet yang telah ditetapkan.

Untuk menjamin keamanan informasi dalam penanganan media penyimpanan informasi, maka kebijakan yang diterapkan adalah sebagai berikut:

a. Informasi yang terkandung dalam media penyimpan informasi yang dapat dipakai ulang dan digunakan sebagai media transit seperti disket dan USB *flash disk* harus dihapus jika tidak diperlukan lagi, namun hanya dilakukan jika salinan asli informasi tersebut masih tersedia;
b. Pegawai yang diminta untuk menghapus dan memindahkan informasi melalui media apapun harus sadar/peduli terhadap Kebijakan Pengelolaan

Keamanan Informasi DJP dan memahami prosedur- prosedur yang harus dijalankan;

c. Seluruh media penyimpan informasi mudah jinjing (*removable*) harus diformat ulang atau dihapus isinya sebelum dibuang. Namun apabila hal itu tidak dapat dilakukan, media tersebut harus dihancurkan;

d. Media kertas termasuk *carbon copies* dan cetakan *printer* yang mengandung informasi rahasia dan sangat rahasia yang tidak diperlukan lagi harus dihancurkan dengan menggunakan alat penghancur kertas atau dibakar;

e. Media lain seperti disket, *tape*, CD, DVD, *USB flash disk*, dan lain-lain, yang tidak diperlukan lagi harus dirusak secara fisik sehingga isinya tidak dapat diakses lagi oleh pihak yang tidak berwenang;

f. Dokumentasi sistem, baik yang tercetak ataupun yang berupa dokumen elektronik digolongkan sebagai dokumen rahasia dan harus disimpan secara aman serta hanya disediakan bagi mereka yang memerlukannya.

Untuk mengamankan informasi dalam pertukaran informasi, kebijakan yang diterapkan adalah sebagai berikut:

a. Pertukaran informasi dan perangkat lunak antara DJP dengan pihak ketiga hanya akan dilakukan atas persetujuan tertulis kedua belah pihak. Khusus untuk pertukaran informasi digital, hal ini hanya dapat dilakukan dengan persetujuan Direktur TIP;

b. Pemilik aset informasi harus menjamin bahwa pertukaran informasi penting dan rawan hanya dilakukan setelah melalui suatu pengkajian risiko yang memadai dan setelah dilakukan penetapan ketentuan- ketentuan keamanan informasi dalam perjanjian pertukaran informasi antara pihak yang terkait;

c. Pegawai DJP harus menghindari pembicaraan menyangkut informasi penting DJP apabila sedang berada atau menelepon di tempat umum;

d. Aset informasi yang dikirim dengan menggunakan jasa layanan kurir atau pos rawan diakses oleh pihak yang tidak berwenang selama pengiriman.

e. Informasi internal DJP yang disediakan bagi masyarakat umum harus disetujui oleh Pemilik Aset Informasi dan harus dilindungi keutuhannya dari modifikasi oleh pihak yang tidak berwenang.

Untuk memantau pelaksanaan pengelolaan keamanan informasi, kebijakan yang diterapkan adalah sebagai berikut:

a. Gangguan keamanan informasi yang ditemukan selama pemantauan harus segera dicatat dan dilaporkan kepada Pejabat Keamanan Informasi terkait;
b. Pejabat Keamanan Informasi harus melakukan evaluasi mendalam terhadap laporan-laporan hasil pemantauan khususnya pada penggunaan yang tidak wajar dari aset-aset informasi yang mungkin merupakan penyalahgunaan aset tersebut;
c. Catatan atau *log* dari sistem informasi tertentu yang bersifat kritikal diaktifkan dan disimpan dengan retensi yang sesuai untuk keperluan pemantauan keamanan sistem dengan memperhatikan tingkat ketersediaan media penyimpanan dan kinerja sistem;
d. Penggunaan sistem informasi yang telah berjalan harus dipantau, dan laporannya digunakan sebagai bahan proyeksi kebutuhan tahun yang akan datang untuk menjamin ketersediaan sistem informasi yang diperlukan; dan
e. Penggunaan sumber daya sistem informasi utama seperti *file server, e-mail server,* dan sistem lainnya yang kritikal bagi kegiatan DJP harus dipantau agar kapasitas tambahan dapat disediakan apabila diperlukan.

Pedoman *Backup* dan *Restore* Sistem/Data/Informasi, Enkripsi dan *Key Management,* Penggunaan *User Account*/*Password* dan Pengamanan *Log-on* ke dalam Fasilitas Teknologi Informasi, Penggunaan Fasilitas *e-Mail*, serta Penggunaan Akses Internet dan Intranet ditetapkan tersendiri dalam Surat Edaran Direktur Jenderal Pajak.

4.6. Pengendalian Akses Terhadap Aset Informasi

Kebijakan Pengendalian Akses Terhadap Aset Informasi ini bertujuan untuk memberi acuan dalam:

a. Mengatur pengelolaan akses dan kewajiban pengguna terhadap aset informasi DJP;
b. Memastikan keabsahan akses pengguna dan mencegah akses pengguna yang tidak berwenang terhadap fasilitas dan aset informasi DJP.
c. Melindungi aset informasi DJP dari serangan virus maupun *malware*.

Kebijakan Pengendalian Akses Terhadap Aset Informasi ini mencakup hal-hal sebagai berikut:

a. Pengelolaan akses pengguna ke aset informasi;
b. Keamanan akses ke jaringan dan sistem informasi DJP;
c. Keamanan akses ke aplikasi dan informasi DJP;
d. Pencegahan serangan *virus* di jaringan dan sistem pengolah informasi DJP;
e. Mobile Computing dan Teleworking;
f. Pedoman Penggunaan *User Account*/*Password* dan Pengamanan *Log-on* ke dalam Fasilitas Teknologi Informasi, Penggunaan Fasilitas *e-Mail*, serta Penggunaan Akses Internet dan Intranet;
g. Pedoman Teleworking;
h. Pedoman Pencegahan *Malware*.

Kebijakan yang berlaku dalam pengelolaan akses pengguna ke aset informasi secara umum adalah sebagai berikut:

a. Hak penggunaan/akses terhadap aset-aset informasi hanya diberikan sesuai dengan kebutuhan tugas dan fungsi pegawai dan diberikan berdasarkan prinsip minimum/seperlunya yaitu cukup untuk memenuhi kebutuhan pegawai dalam menjalankan tugasnya;
b. Setiap permintaan hak penggunaan/akses oleh pegawai DJP harus disetujui oleh atasan pegawai yang bersangkutan minimal setingkat Eselon III;
c. Hak akses khusus, yakni hak untuk menggunakan akses ke dalam sistem informasi yang mengolah data/informasi yang bersifat rahasia dan sangat rahasia termasuk didalamnya namun tidak terbatas pada sistem operasi, *storage devices*, file server, dan aplikasi-aplikasi, hanya dapat diberikan kepada pengguna yang terlatih;
d. Hak akses khusus hanya dapat digunakan untuk melakukan pekerjaan yang hanya dapat dilaksanakan melalui *account* akses khusus.

Untuk menjamin keamanan akses ke jaringan dan sistem informasi DJP, maka diterapkan kebijakan sebagai berikut:

a. Akses ke jaringan milik DJP hanya boleh diberikan kepada pengguna yang berwenang;
b. Untuk menghindari akses oleh pihak yang tidak berwenang, pemberian akses dilakukan melalui proses *log-on* yang aman. Pada saat log-on sistem tidak mengungkapkan informasi apapun yang dapat dimanfaatkan oleh pihak yang tidak berwenang untuk mendapatkan akses ke jaringan;
c. Interaksi antara pengguna dengan sistem operasi perangkat pengolah informasi hanya diperkenankan sebatas fungsi-fungsi dan aplikasi- aplikasi sistem yang diperlukan untuk melaksanakan pekerjaan. Proses otorisasi/pemberian ijin akses terhadap sistem operasi harus didefinisikan secara tepat dan jelas;
d. Penggunaan alat bantu sistem (*system utilities*) harus dibatasi dan hanya diberikan kepada pengguna yang tugasnya memerlukan fasilitas *system utilities* tersebut.

Untuk menjamin keamanan akses ke aplikasi dan informasi DJP, maka diterapkan kebijakan sebagai berikut:

a. Komputer yang menyimpan informasi penting dan rawan yang dikelola DJP harus ditempatkan di lokasi yang terpisah dari area publik untuk mencegah akses pihak yang tidak berwenang; dan
b. Pemantauan keamanan atas penggunaan akses ke aplikasi dan informasi DJP dilakukan oleh pengguna sebagai pemilik akses, administrator sistem, dan Petugas Keamanan Informasi terkait.

Untuk mencegah serangan virus dan *malware* di jaringan dan sistem pengolah informasi DJP, maka diterapkan kebijakan sebagai berikut:

a. Perangkat lunak antivirus dan *malware* harus dipasang di setiap komputer pengguna untuk menghalangi masuknya *virus* ke dalam komputer;
b. Pengguna harus memberitahu *Service Desk* TIK apabila mendeteksi adanya virus atau *malware*, terjadi perubahan konfigurasi secara tiba-tiba, atau adanya perilaku aplikasi dan/atau komputer yang menyimpang; dan

c. Kemampuan pengguna dalam pencegahan dan penghapusan virus akan ditingkatkan melalui pelatihan, sosialisasi, dan tindakan-tindakan praktis untuk mencegah atau menghilangkan virus.

Dalam penyelenggaraan *mobile computing* dan *teleworking*, diterapkan kebijakan sebagai berikut:

a. Fasilitas *mobile computing* yang disediakan oleh DJP hanya dapat dipergunakan untuk melaksanakan tugas dan fungsi DJP dan harus mendapat persetujuan dari Pejabat Keamanan Informasi terkait;
b. Pegawai yang menerima fasilitas *mobile computing* DJP harus menjamin bahwa akses ke perangkat tersebut terlindung dari akses oleh pihak yang tidak berwenang;
c. Pejabat Keamanan Informasi memastikan bahwa pegawai yang menggunakan fasilitas *mobile computing* mendapatkan pelatihan yang memadai, dan pegawai yang bersangkutan harus sadar akan risiko-risiko keamanan yang terus meningkat terhadap informasi yang disimpan dalam peralatan-peralatan yang digunakan.

Pedoman Penggunaan *User Account*/*Password* dan Pengamanan *Log-on* ke dalam Fasilitas Teknologi Informasi, Penggunaan Fasilitas *e-Mail*, serta Penggunaan Akses Internet dan Intranet, Pedoman *Teleworking,* Pedoman Pencegahan *Malware* akan ditetapkan tersendiri dalam Surat Edaran Direktur Jenderal Pajak.

4.7. **Keamanan Informasi Dalam Pengembangan Dan Pemeliharaan Sistem Informasi**

Kebijakan Keamanan Informasi dalam Pengembangan dan Pemeliharaan Sistem Informasi ini bertujuan untuk memberikan acuan dalam memastikan keamanan informasi dalam pengolahan data dalam perangkat lunak atau aplikasi dan menjamin keamanan informasi dan integritas data dalam pengelolaan *end-user computing*.

Kebijakan Keamanan Informasi dalam Pengembangan dan Pemeliharaan Sistem Informasi ini mencakup hal-hal sebagai berikut:

a. Ketentuan mengenai pengolahan data dalam perangkat lunak/aplikasi;

b. Penggunaan enkripsi;
c. Pengamanan arsip (*files*) pendukung kinerja sistem;
d. Pengelolaan end user computing;
e. Proses pengembangan maupun operasional sistem informasi;
f. Pedoman Enkripsi dan *Key Management.*

Pengolahan data dalam perangkat lunak/aplikasi harus memenuhi ketentuan sebagai berikut:

a. Data yang dimasukkan ke aplikasi apapun secara manual harus diperiksa terlebih dahulu kebenaran dan kesesuaiannya;
b. Semua bentuk data *input* atau *output* yang dibutuhkan atau dihasilkan oleh suatu aplikasi harus diverifikasi terlebih dahulu untuk memastikan bahwa bentuk/format datanya sesuai dengan spesifikasi yang ditetapkan untuk kebutuhan aplikasi tersebut;
c. Setiap aplikasi harus mempunyai fitur yang dapat mengidentifikasi dan memberitahukan adanya perubahan data yang disebabkan oleh adanya kesalahan pemrosesan data atau oleh adanya percobaan intrusi;
d. Setiap aplikasi harus mempunyai fitur pengaman yang dapat melindungi otentikasi dan integritas data dalam pemrosesannya, termasuk dalam proses pertukaran data dengan aplikasi lain, di mana spesifikasinya telah disesuaikan dengan kebutuhan atau klasifikasi data yang terkait;
e. Pada setiap aplikasi harus disertakan proses validasi data untuk menjamin bahwa informasi yang dihasilkan sesuai dengan yang diharapkan penggunanya dan sesuai dengan klasifikasi penggunaannya;
f. Apabila aplikasi gagal memberikan hasil yang diharapkan, sistem harus dapat memunculkan pemberitahuan pesan atau petunjuk kegagalannya.

Kebijakan yang berlaku dalam penggunaan enkripsi adalah sebagai berikut:

a. Data yang sensitif dan berisiko tinggi harus diamankan secara ketat, dan apabila perlu dilakukan perlindungan secara enkripsi bila ditransfer melalui *e-mail* atau jaringan;
b. Kajian dan penyusunan standar yang tepat dalam penerapan enkripsi dilakukan sebelum penerapan penggunaan sistem untuk proses enkripsi;

c. Sistem dan teknik enkripsi hanya digunakan untuk melindungi informasi yang berisiko tinggi, dan penggunaannya harus mendapat ijin dari Pejabat Keamanan Informasi Direktorat TIP.

Untuk mendukung pengamanan arsip (*files*) pendukung kinerja sistem diterapkan kebijakan sebagai berikut:

a. Akses terhadap arsip-arsip pendukung kinerja sistem (*system files*) dibatasi hanya untuk pegawai DJP yang bertanggung jawab dalam pengelolaan *server*;
b. Proses pemutakhiran (*update*) perangkat lunak operasional hanya boleh dilakukan oleh pegawai yang berwenang melalui Pedoman Pengelolaan Perubahan yang akan diatur tersendiri dalam Kebijakan Pengelolaan Layanan TIK;
c. Catatan kejadian dan perlakuan terhadap sistem (*audit log*) selama proses pemutakhiran harus disimpan dan dirawat dengan baik;
d. Salinan versi terkini dari perangkat lunak yang akan dimutakhirkan harus disimpan di tempat yang aman sebagai antisipasi terhadap keadaan yang tidak dikehendaki.

Untuk menjamin keamanan informasi dan integritas data dalam hal pengelolaan *end user computing*, maka kebijakan yang diterapkan adalah sebagai berikut:

a. Ketua Tim Keamanan Informasi DJP memastikan terdapat pembagian peran dan tanggung jawab dalam pengelolaan *end user computing*, dimana terdapat pemisahan fungsi yang menjalankan kegiatan analisis kebutuhan akan *end user computing*, *approval* pengembangan, pelaksanaan pengembangan, dan evaluasi atas *end user computing;*
b. Pengguna tidak diperkenankan mengembangkan aplikasi yang digunakan untuk melakukan transaksi bisnis DJP, kecuali untuk mengembangkan aplikasi yang bertujuan untuk membantu analisis kegiatan operasional sehari-hari;

Untuk menjamin keamanan informasi dalam proses pengembangan maupun operasional sistem informasi diterapkan kebijakan sebagai berikut:

a. Lingkungan *development*/pengembangan dan operasional sistem informasi harus dipisahkan baik secara fisik, *logic*, maupun aksesnya;
b. Spesifikasi perangkat lunak baik yang dikembangkan sendiri oleh internal maupun oleh pihak ketiga harus didokumentasikan secara formal;
c. Jika sistem operasi yang digunakan diubah, maka aplikasi yang berjalan di atasnya harus dievaluasi dan diuji kembali untuk menjamin keutuhan sistemnya tidak terganggu;
d. Setiap paket perangkat lunak yang dikembangkan oleh pihak ketiga yang digunakan dalam sistem informasi milik DJP harus bebas dari mekanisme deaktivasi (pemberhentian atau penidakaktifan operasi/layanan) yang dapat dipicu oleh pihak ketiga tersebut tanpa sepengetahuan DJP;
e. Kelemahan-kelemahan teknis sistem informasi yang digunakan harus segera diidentifikasi, dikaji risikonya, dan ditetapkan kontrol-kontrolnya untuk mencegah atau menutup kelemahan-kelemahan yang terjadi;
f. Pengembangan perangkat lunak yang dilakukan oleh pihak ketiga harus diawasi dan dipantau untuk memastikan bahwa proses pengembangannya memenuhi syarat-syarat keamanan informasi yang ditetapkan dalam kontrak;
g. Data yang digunakan dalam pengujian sistem (*system-testing data*) harus dilindungi dari kemungkinan rusak, hilang, atau perubahan yang dilakukan tanpa ijin;
h. Akses terhadap program *source library* harus dikendalikan secara ketat untuk mengurangi kemungkinan rusak, baik secara sengaja maupun tidak.

Pedoman Enkripsi dan *Key Management* akan ditetapkan tersendiri dalam Surat Edaran Direktur Jenderal Pajak, yang antara lain akan mengatur pengembangan dan penerapan enkripsi untuk melindungi informasi serta penerapan *Key Management* untuk mendukung penggunaan teknik-teknik enkripsi di DJP.

4.8. **Pengelolaan Gangguan Keamanan Informasi**

Kebijakan Pengelolaan Gangguan Keamanan Informasi ini bertujuan untuk memberikan acuan dalam mengelola penanganan terhadap gangguan

keamanan informasi yang terjadi di lingkungan DJP dan memastikan pengambilan tindakan perbaikan secara cepat dan tepat terhadap peristiwa dan kelemahan keamanan infomasi yang berkaitan dengan sistem informasi melalui proses komunikasi efektif antar pihak-pihak yang bertanggung jawab.

Kebijakan Pengelolaan Gangguan Keamanan Informasi ini mencakup hal-hal sebagai berikut:

a. Pelaporan kelemahan atau gangguan/insiden keamanan informasi;
b. Evaluasi gangguan/insiden keamanan informasi;
c. Pencatatan dan pengamanan data dan rekaman pelaporan gangguan/insiden keamanan informasi;
d. Pedoman Pengelolaan Gangguan Keamanan Informasi.

Seluruh pegawai dan pihak ketiga harus melaporkan sesegera mungkin ke *Service Desk* TIK baik secara langsung maupun melalui *Operator Console* atau pegawai yang ditunjuk apabila menemukan kelemahan atau menjumpai terjadinya gangguan/insiden keamanan informasi.

Tim keamanan informasi bertanggung jawab untuk mengevaluasi gangguan/insiden keamanan informasi secara berkala untuk menjamin adanya pengelolaan keamanan informasi yang efektif, memeriksa tindakan-tindakan pencegahan yang telah dilakukan, dan merencanakan cara deteksi awal terhadap terjadinya insiden keamanan informasi.

Kepedulian pengguna (*user*) terhadap kelemahan keamanan informasi akan ditingkatkan melalui kegiatan sosialisasi dan pelatihan.

Unit kerja TIK bertanggung jawab untuk menyediakan perangkat kerja dalam menindaklanjuti dan menyelesaikan setiap pelaporan insiden keamanan informasi secara cepat dan efektif.

Seluruh gangguan/insiden keamanan informasi yang terjadi dan tindakan untuk mengatasi gangguan/insiden tersebut akan dicatat dalam suatu basis data pelaporan insiden keamanan informasi, dan akan menjadi masukan dalam evaluasi pengelolaan keamanan informasi.

Unit kerja TIK bertanggung jawab untuk mengevaluasi laporan dan penyelesaian insiden keamanan informasi untuk mengidentifikasi jenis dan volume insiden yang terkait dalam rangka pengawasan dan evaluasi kinerja Tim Keamanan Informasi.

Semua data dan rekaman yang dibutuhkan untuk menganalisis dan menyelesaikan insiden keamanan informasi harus diamankan. Untuk insiden yang terkait dengan tindakan perdata atau pidana, pengamanan data dan rekaman harus mengikuti peraturan dan hukum yang berlaku.

4.9. Keamanan Informasi Dalam Pengelolaan Kelangsungan Layanan TIK

Kebijakan Keamanan Informasi dalam Pengelolaan Kelangsungan Layanan TIK ini bertujuan untuk memberikan acuan dalam mengatasi gangguan terhadap kegiatan kerja, melindungi proses kerja yang vital dari dampak kegagalan sistem informasi atau bencana dan untuk memastikan proses kembali ke keadaan normal dalam waktu yang tidak terlalu lama.

Kebijakan Keamanan Informasi dalam Pengelolaan Kelangsungan Layanan TIK ini mencakup hal-hal yang menjadi pertimbangan untuk dikembangkan di dalam Kebijakan Pengelolaan Kelangsungan Layanan TIK.

Pengelolaan Kelangsungan Layanan TIK bagi seluruh proses kegiatan vital yang terkait layanan berbasis TIK dalam rangka mengurangi dampak kegagalan sistem informasi atau bencana yang menyebabkan terganggunya kegiatan DJP akan mengacu kepada Kebijakan Pengelolaan Kelangsungan Layanan TIK.

Pengelolaan keamanan informasi yang terkait dalam kelangsungan layanan TIK dilakukan dengan mempertimbangkan hal-hal sebagai berikut:

a. Identifikasi aset-aset informasi yang vital dan sensitif, khususnya aset informasi dengan klasifikasi sangat rahasia dan rahasia;
b. Identifikasi kejadian-kejadian yang menyebabkan gangguan tehadap proses kegiatan yang penting;
c. Tindak lanjut terhadap hasil kajian risiko keamanan informasi; dan
d. Pengelolaan ini merupakan bagian yang tidak terpisahkan dari *Business Continuity Management* DJP secara keseluruhan.

4.10. Kepatuhan

Kebijakan Kepatuhan ini bertujuan untuk memberikan acuan dalam mencegah pelanggaran terhadap segala undang-undang, ketentuan, dan peraturan mengenai keamanan informasi.

Kebijakan Keamanan Informasi dalam Pengelolaan Kelangsungan Layanan TIK ini mencakup hal-hal sebagai berikut:

a. Peningkatan kepatuhan terhadap kebijakan, pedoman, prosedur, dan standar keamanan informasi;
b. Penggunaan lisensi dan kepemilikan hak cipta (HAKI);
c. Pemeriksaan terhadap kepatuhan;
d. Audit terhadap sistem informasi;
e. Pedoman Audit Internal Tata Kelola TIK

Seluruh pengguna (*user*) sistem informasi milik DJP termasuk pihak ketiga harus mematuhi Kebijakan Pengelolaan Keamanan Informasi ini, menaati ketentuan hukum dan perundang-undangan yang terkait, serta mentaati perjanjian tentang lisensi, termasuk persyaratan-persyaratan kontrak yang telah disetujui.

Setiap ketidakpatuhan terhadap kebijakan, prosedur, dan standar keamanan informasi harus dicari penyebab utamanya dan ditindaklanjuti untuk mencegah terjadinya hal serupa di kemudian hari.

Seluruh pegawai DJP dan pihak ketiga dilarang menggunakan perangkat lunak untuk menggandakan atau menggunakan lisensi secara tidak sah, untuk melacak dan menemukan *password*, untuk mengidentifikasi kelemahan keamanan informasi, atau untuk membuka enkripsi *file* dan/atau perangkat keras yang dapat dioperasikan untuk mengevaluasi atau menerobos keamanan sistem informasi, kecuali mendapat ijin dan diberi wewenang oleh Pejabat Keamanan Informasi terkait.

Selanjutnya sebagai pedoman pelaksanaan PER - 41/PJ/2010 yang selanjutnya disebut Buku Dua ini, disusun Kebijakan Keamanan Informasi ini dengan struktur sebagai berikut :

Tabel 2.1 Struktur Kebijakan Pengelolaan Keamanan Informasi DJP

No.	Peraturan	Nomor Peraturan
1.	**Kebijakan Pengelolaan Keamanan Informasi DJP**	**PER-41/PJ/2010**
2.	Pedoman Pengelolaan User Account, e-Mail, Internet, Intranet	SE-136/PJ/2010
3.	Pedoman Pengendalian Dokumen & Catatan Penerapan Tata Kelola TIK	SE-10/PJ/2011
4.	Pedoman Akses Pihak Ketiga	SE-159/PJ/2010
5.	Pedoman Backup dan Restore Sistem/Data/Informasi	SE-52/PJ/2011
6.	Pedoman Pengelolaan Aset Informasi	SE-57/PJ/2011
7.	Pedoman Pencegahan *Malware*	SE-15/PJ/2011
8.	Pedoman Pengamanan Perangkat dan Fasilitas Pengolahan Data/Informasi	SE-16/PJ/2011
9.	Pedoman Pengelolaan HAKI	SE-12/PJ/2011
10.	Pedoman Teleworking	SE-61/PJ/2011
11.	Pedoman Enkripsi dan Key Management	SE-56/PJ/2011
12.	Pedoman Tindakan Perbaikan & Pencegahan, serta Pengelolaan Gangguan Keamanan Informasi	SE-9/PJ/2011
13.	Pedoman Audit Internal Tata Kelola TIK	SE-5/PJ/2011
14.	Pedoman Tinjauan Manajemen Pengelolaan Keamanan Informasi	SE-14/PJ/2011

Terkait Aset dan Perangkat terdapat beberapa Kewajiban yang harus dilaksanakan seluruh pegawai dan larangan yang harus patuhi pegawai, yaitu :

- Menjaga keamanan informasi yang menjadi tanggung jawabnya
- Menjamin bahwa aset informasi dan sistem pengamanannya tersedia, terawat dan berfungsi dengan baik .
- Menggunakan perangkat Komputer sebaik-baiknya, dengan memperhatikan kebersihan, keamanan, dan kepentingan penggunaan jangka panjang.
- Memasang *password* pada perangkat komputer yang berisikan informasi rahasia dan sangat rahasia.
- Mencegah kerusakan pada perangkat komputer.
- Dapat memastikan bahwa perangkat lunak yang terpasang di perangkat komputer miliknya merupakan perangkat lunak legal/berlisensi
- Perangkat komputer harus berada dalam kondisi terjaga/di bawah pengawasan pengguna aset informasi
- Apabila perangkat komputer membutuhkan perbaikan/perawatan, data yang bersifat kritikal harus dipindahkan dan diamankan.
- Setiap pegawai DJP harus mengidentifikasi data-data yang dianggap penting pada perangkat komputer masing-masing

- Setiap pegawai harus memiliki media backup yang sesuai. Media yang dapat digunakan antara lain: removable media, CD, DVD, Harddisk eksternal, dan sebagainya
- Pegawai DJP harus menyimpan lebih dari satu salinan data yang penting dengan interval waktu yang berbeda untuk mencegah kehilangan atau kerusakan data.
- Salinan dari media backup dan catatan tentang data yang dibackup harus disimpan secara aman, misalnya dalam lemari terkunci.
- Pegawai DJP harus memastikan bahwa backup dilakukan dengan benar.

Di samping itu terdapat larangan bagi pegawai DJP, yaitu :

- Melakukan instalasi atau menghapus sendiri perangkat lunak di fasilitas pengolah informasi milik DJP
- Membuka/membongkar perangkat komputer seperti CPU, monitor, keyboard, mouse, dan lain-lain.
- Meninggalkan Layar (monitor) PC dan Notebook dalam keadaan tidak terkunci (ter-password).
- Perangkat komputer tidak boleh digunakan kepentingan pribadi

Terkait Pengelolaan User Account dan Password terdapat beberapa kewajiban:

- Menjaga kerahasiaan password.
- Segera mengganti password apabila sudah diketahui orang lain.
- Memasang screensaver yang dilindungi password pada komputer yang menjadi tanggung jawabnya (otomatis aktif dengan setelah komputer tidak digunakan selama 10 menit).
- Melakukan proses logoff apabila telah selesai menggunakan atau akan meninggalkan fasilitas teknologi informasi.
- Mengaktifkan konfigurasi yang akan mematikan perangkat komputer setelah 30 menit tidak digunakan.

Terkait Pengelolaan User Account dan Password terdapat beberapa larangan Pemilik User Account :

- Memberitahukan *password*nya kepada siapa pun

- Menggunakan password yang sama antara fasilitas TIK DJP dengan di luar fasilitas DJP
- Menuliskan password pada media apa pun sehingga dapat diketahui orang lain.
- Menggunakan fasilitas *remember password* untuk mengakses aset TIK DJP.

Terkait penggunaan email DJP terdapat beberapa hal yangperlu diperhatikan oleh seluruh pegawai:

Setiap pengguna harus melakukan pengelolaan *e-mail* untuk menghindari gangguan karena kapasitas *mailbox* yang terbatas. Contoh: Menghapus *e-mail* lama yang sudah tidak diperlukan.

Hal-Hal yang harus diperhatikan pada saat mengirim/menerima E-mail :

- kebenaran informasi dalam *e-mail*
- ketepatan alamat para penerima *e-mail*
- seluruh bagian dari *e-mail* dan *attachment* terbebas dari segala program/aplikasi yang dapat merusak dan merugikan.
- melakukan verifikasi kebenaran informasi pada *e-mail* yang diterima .
- memastikan bahwa *e-mail* bebas *malware* sebelum menggunakan informasi yang diperoleh.

Dalam mengirim/menerima E-mail terdapat beberapa :

- Mengirimkan *e-mail* atas nama orang lain.
- Mengirimkan *e-mail* yang isinya bertentangan dengan hukum dan perundang-undangan yang berlaku di negara Republik Indonesia
- Menggunakan alamat *e-mail* DJP di Internet, misalnya untuk keperluan pembelian barang, mendaftar ke jejaring sosial, mendaftar ke milis, dsb.
- Mengirimkan *e-mail* berisikan ancaman, penghinaan, caci-maki, kata-kata kasar, fitnah, hasutan, atau pencemaran nama baik orang lain, atau berisikan pandangan dan pendapat pribadi terhadap sesama pegawai, pimpinan, mitra, atau pihak lainnya yang terkait dengan DJP ataupun yang terkait dengan isu politik.
- Mengirim secara otomatis (*automatic forwarding*) *e-mail* yang diterimanya melalui alamat *e-mail* DJP untuk mencegah terjadinya kebocoran informasi kepada pihak-pihak yang tidak berwenang.

- Mengirimkan salinan (Cc/Bcc) *e-mail*-nya ke alamat-alamat *e-mail* di luar DJP kecuali jika sesuai dengan tugas, fungsi, dan wewenang jabatannya.
- Mengirimkan *e-mail* berantai (*chain e-mail*) dengan menggunakan alamat *e-mail* DJP.

Penggunaan E-Mail Signature juga diatur sebagai berikut :

- Setiap pengguna harus mencantumkan identitas diri atau *e-mail signature* pada setiap *e-mail* yang dikirimkannya dengan memanfaatkan fasilitas *setting signature* otomatis yang tersedia.

Tabel 2.2 Format *Email Signature*

Format E-mail Signature
***<nama lengkap>* (font Calibri, 11, bold)**
<nama jabatan dan nama unit eselon IV> (Calibri, 11, italic)
<nama unit eselon III> (Calibri, 11, italic)
<nama unit eselon II> (Calibri, 11, italic)
<nama unit eselon I> (Calibri, 11, italic)
<alamat> (Calibri, 11, italic)
<kota dan kode pos> (Calibri, 11, italic)
<nomor telepon/fax> (Calibri, 11, italic)

Bagi Pejabat Fungsional, setelah nama lengkap langsung diikuti dengan nama unit atasan langsungnya

Eko Budi
Pemeriksa Pajak Pertama
KPP Pratama Jakarta Mampang
Kantor Wilayah Direktorat Jenderal Pajak Jakarta Selatan
Jl. Raya Pasar Minggu No.1
Jakarta Selatan 12780
Telp. (021) 79191232, 7949574
Fax. (021) 7991035, 7949575

Pejabat Eselon III dan Pejabat Eselon II tidak perlu menyebutkan unit eselon di bawahnya tetapi menggabungkan nama jabatan dengan nama Unit Eselon III atau Unit Eselon II-nya

Ahmad Joko
Kepala KPP Pratama Jakarta Mampang
Kantor Wilayah Direktorat Jenderal Pajak Jakarta Selatan
Jl. Raya Pasar Minggu No.1
Jakarta Selatan 12780
Telp. (021) 79191232, 7949574
Fax. (021) 7991035, 7949575

Terkait penggunaan internet terdapat beberapa hal yang perlu diperhatikan oleh seluruh pegawai:

Dalam Menggunakan Fasilitas Internet, Pegawai DJP tidak diperkenankan untuk:

- Mengunduh *file*/data/informasi/perangkat lunak dari Internet atau menjalankan program/aplikasi dari Internet kecuali apabila tidak bertentangan dengan kebijakan dan prosedur keamanan informasi yang berlaku di DJP.
- Mengunggah, mengunduh, dan/atau menjalankan perangkat lunak berlisensi milik DJP untuk keperluan di luar DJP.

- Menggunakan aplikasi percakapan elektronik (*chatting* atau *instant messaging*) yang disediakan melalui Internet.
- Mengunduh dan berbagi akses (*sharing*) arsip-arsip audio (MP3, WAV, dsb), video (AVI, DIVX, MKV, atau dalam bentuk *video streaming*), dan foto digital kecuali untuk kepentingan DJP.
- Menggunakan modem/perangkat akses internet selain yang disediakan oleh DJP dan terhubung dengan jaringan lokal (LAN).
- Melewati (*bypass*) perangkat pengendalian/pembatasan akses Internet yang digunakan DJP, mematikan atau menghindari perlindungan antivirus yang digunakan DJP.
- Mengungkapkan atau menyebarkan informasi milik DJP dengan klasifikasi selain Publik melalui fasilitas Internet.
- Menggunakan akses Internet untuk melakukan aktivitas yang bertentangan dengan hukum dan undang-undang yang berlaku di Republik Indonesia dan/atau menggunakan hak atas kekayaan intelektual pihak lain tanpa persetujuan pihak berwenang melalui fasilitas Internet DJP.
- Menggunakan fasilitas Internet yang disediakan DJP untuk melancarkan aktivitas *hacking*/serangan terhadap fasilitas teknologi informasi baik milik DJP maupun milik orang/badan hukum lainnya.
- Menyebarkan/menempatkan di Internet informasi/tulisan yang berisikan hal-hal negatif.

Contoh: ancaman, penghinaan, caci-maki, kata-kata kasar, fitnah, hasutan atau pencemaran nama baik orang lain, pandangan dan pendapat pribadi baik positif maupun negatif, termasuk isu politik, terhadap sesama pegawai, pimpinan, mitra, dan pihak lainnya yang terkait dengan DJP.

Terkait penanganan *Malicious Software* (Malware) terdapat beberapa hal yang perlu diperhatikan oleh seluruh pegawai:

- Memindai *removable media* pada perangkat komputer sebelum digunakan.
- Menyimpan lampiran (*attachment*) e-mail ke dalam komputer lokal dan memindai sebelum membukanya.
- Mengunduh dan menginstalasi anti *malware* terbaru pada komputer yang digunakan. Anti malware diperoleh dari PortalDJP.

- Apabila ditemukan indikasi gangguan *malware*, segera memutuskan koneksi perangkat komputer dari jaringan DJP dan melapor kepada OC atau administrator sistem di unit kerja masing-masing.

Untuk Mencegah Gangguan akibat Malware, Pegawai DJP tidak diperkenankan untuk:

- Mengirim atau menerima file berbentuk *active content* atau executable file, yaitu file-file dengan ekstensi .exe, .hlp, .scr, .asp dan sebagainya melalui e-mail
- Menyalin, mengunduh, membuka, atau menginstalasi file dari sumber atau *removable media* yang mencurigakan atau tidak terpercaya
- Mengunjungi situs berisi konten mencurigakan yang disinyalir dapat menyebarkan *malware*.
- Mengubah konfigurasi perangkat jaringan tanpa persetujuan dari pejabat yang berwenang
- Menonaktifkan perangkat/fasilitas anti malware
- Membuka pop up windows yang tidak dikenal atau yang mencurigakan.

Dalam hal terjadi gangguan *malware*, hal-hal yang harus dilakukan Pegawai DJP:

- Melakukan langkah-langkah sebagaimana terdapat dalam buku panduan penanganan malware yang diterbitkan oleh Direktorat TIP
- Apabila pegawai tetap tidak dapat menyelesaikan gangguan tersebut, pegawai harus melapor kepada Operator Console atau Pegawai yang ditunjuk oleh Pimpinan Unit Kerja.

Penanganan Gangguan malware selanjutnya mengikuti langkah-langkah penyelesaian Gangguan keamanan informasi.

Terkait penanganan Gangguan Keamanan Informasi terdapat beberapa hal yang perlu diperhatikan dan dilakukan oleh seluruh pegawai:

- Pegawai DJP harus tanggap terhadap ketidaksesuaian yang terjadi di unit kerjanya masing-masing untuk membantu mengamankan aset informasi DJP.

- Pegawai DJP yang melihat/mendengar/menerima keluhan terjadinya pelanggaran terhadap kebijakan Pengelolaan Keamanan Informasi harus melaporkannya kepada atasan atau Pejabat Keamanan Informasi terkait.
- Pegawai DJP yang menemukan terjadinya gangguan keamanan informasi harus mencatat gangguan tersebut untuk dilaporkan kepada Pejabat Keamanan Informasi.

Insiden/Gangguan Keamanan Informasi yang harus dilaporkan antara lain:

- Pengungkapan, perubahan, penghancuran aset informasi milik DJP
- Usaha pihak tidak berwenang untuk mendapatkan akses ke aset informasi DJP
- Kehilangan/pencurian aset informasi DJP, termasuk diantaranya kunci enkripsi dan password.

Terkait Keamanan Fisik dan Lingkungan terdapat beberapa hal yang perlu diperhatikan dan dilakukan oleh seluruh pegawai:

1. Ruang Server
    - Ruang server hendaknya berada pada lokasi yang:
        - Terbatas untuk publik (*restricted area*)
        - Mudah diawasi
        - Aman dari bahaya genangan air (misalnya dekat dengan kamar mandi)
    - Lokasi Ruang server tidak boleh dicantumkan pada papan nama/papan penunjuk
    - Ruang server harus tertutup, dan dinding ruangan harus terbuat dari material yang tidak dapat dilihat dari luar
    - Lokasi di sekitar ruang server harus diberi penerangan yang memadai
    - Terdapat alat penerangan darurat yang dapat mencakup seluruh area ruang server
    - Tersedia alarm api dan asap, alat pengukur suhu dan kelembaban, perangkat pengawasan video
    - Pemadam api berbasis air tidak boleh digunakan di ruang server
    - Ruang Server harus dilengkapi pintu elektronik, sistem pemadam kebakaran, alarm bahaya, dan perangkat pemutus aliran listrik.

- Perangkat dan fasilitas pengolahan data dan informasi (storage, router, jaringan kabel, dan sebagainya) ditempatkan di area yang hanya bisa diakses petugas yang berwenang
- Setiap kabel harus diberi label yang sesuai, jelas, dan teratur
- Jaringan kabel data harus dipisahkan dari jaringan kabel listrik dengan jarak minimal 3 meter.
- Dalam hal terdapat *raised floor*, jaringan kabel data diletakkan ditempatkan di jalur khusus di atas plafon sedangkan jaringan kabel listrik berada di bawah raised floor.
- Ketersediaan, perawatan, pemeliharaan, pemeriksaan, dan pengujian secara berkala dibuktikan dengan bukti rekaman kegiatan dan checklist.

Perangkat Pendukung Ruang Server

- *Uninterruptible Power Supply* (UPS) yang memiliki kapasitas cukup untuk memasok listrik selama minimal 15 menit untuk semua perangkat komputer di ruang server pada saat terjadi gangguan sumber listrik.
- Selain perangkat dan fasilitas pengolah data dan informasi tidak boleh dihubungkan dengan perangkat UPS
- Generator listrik untuk mengatur pasokan daya otomatis dengan kapasitas yang cukup untuk seluruh perangkat komputer dan fasilitas pendukungnya (server, router, printer, AC di ruang server)
- *Air Conditioning System*. Suhu udara diatur dalam batas 20-25^{o}C dengan kelembaban relatif 40-55%
- Fasilitas pemadam api yang mampu memadamkan api kurang dari 2 menit.

2. Akses ke Ruang Server

- Akses keluar masuk harus dibatasi dan hanya diberikan kepada petugas yang berwenang seperti Operator Console dan Administrator Sistem
- Setiap orang selain petugas yang berwenang harus didampingi petugas ruang server saat melakukan akses ke ruang server dan mengisi buku Log.

Larangan

- Makan/Minum/Merokok di Ruang Server
- Menggunakan Ruang Server sebagai ruang kerja

- Menggunakan ruang server untuk tempat menyimpan berkas, perangkat rusak, serta barang-barang lain yang tidak semestinya
- Membawa material mudah terbakar, perangkat elektromagnetik, perangkat telekomunikasi, dan material berbahaya lainnya.
- Mencantumkan lokasi Ruang Server pada papan nama/papan penunjuk

5. Kebijakan Pengelolaan Layanan TIK

Layanan TIK, adalah fasilitas yang terdiri dari gabungan komponen teknologi, proses, dan personil dalam rangka penyelenggaraan sistem informasi yang direncanakan, dikembangkan, dioperasikan, dan dipelihara oleh Unit Kerja TIK DJP baik secara terpusat maupun terdistribusi, yang digunakan untuk memenuhi kepentingan pemenuhan tugas dan fungsi unit kerja terkait maupun DJP pada umumnya.

Unit Kerja TIK adalah Direktorat Transformasi Teknologi Komunikasi dan Informasi dan Direktorat Teknologi Informasi Perpajakan.

Kebijakan Pengelolaan Layanan Teknologi Informasi dan Komunikasi DJP disusun dengan tujuan untuk memberikan acuan yang jelas bagi Direktorat Transformasi Teknologi Komunikasi dan Informasi (TTKI) dan Direktorat Teknologi Informasi Perpajakan (TIP) untuk mengelola Layanan TIK yang berkualitas.

Materi yang diatur dalam Buku Tiga ini meliputi:

a. Pengelolaan Tingkat Layanan TIK;
b. Pengelolaan Pihak Ketiga Penyedia Barang/Jasa TIK;
c. Pengelolaan Kapasitas Layanan TIK;
d. Pengelolaan Ketersediaan Layanan TIK;
e. Service Desk TIK;
f. Pengelolaan Gangguan Layanan TIK;
g. Pengelolaan Problem Layanan TIK;
h. Pengelolaan Aset dan Konfigurasi Layanan TIK;
i. Pengelolaan Perubahan Layanan TIK; dan
j. Penqelolaan *Release* Layanan TIK.

5.1. Pengelolaan Tingkat Layanan TIK

Kebijakan Pengelolan Tingkat Layanan TIK (*IT Service Level Management*) ini disusun dengan tujuan untuk memberikan acuan yang jelas bagi penyedia Layanan TIK (Direktorat TTKI dan Direktorat TIP) dan pengguna Layanan TIK untuk mendefinisikan, menyepakati, dan mengelola tingkat Layanan TIK dalam rangka mencapai sasaran tingkat layanan yang disepakati.

Kebijakan Pengelolaan Tingkat Layanan TIK DJP ini mencakup hal-hal sebagai berikut:

a. Proses-proses dalam rangka menjaga dan meningkatkan kualitas tingkat layanan;
b. Pengaturan mengenai tingkat Layanan TIK/ Service Level;
c. Pengaturan mengenai Katalog Layanan TIK/ IT Service Catalog
d. Pengaturan dalam pemantauan dan pelaporan pencapaian tingkat Layanan TIK;
e. Pengaturan mengenai Pedoman Pengelolaan Tingkat Layanan TIK; dan
f. Pengaturan mengenai peran dan tanggung jawab pihak-pihak yang terkait dalam pengelolaan Layanan TIK.

5.2. **Pengelolaan Pihak Ketiga Penyedia Barang/Jasa TIK**

Kebijakan Pengelolaan Pihak Ketiga Penyedia Barang/Jasa TIK ini disusun untuk memberi acuan bagi Direktorat TTKI dan Direktorat TIP dalam rangka mengelola Pihak Ketiga Penyedia Barang/Jasa TIK agar memberikan layanan yang berkualitas bagi DJP.

Kebijakan ini berlaku bagi unit kerja TIK dalam mengelola penyedia barang/jasa TIK yang memiliki perjanjian kerjasama dengan DJP, maupun yang masih memiliki kewajiban/tanggung jawab/support terhadap DJP pada masa garansi/retensi/pendampingan/transisi atau bentuk kerjasama lainnya.

Kebijakan pengelolaan Pihak Ketiga Penyedia Barang/Jasa TIK ini mencakup hal-hal sebagai berikut:

a. Ketentuan dalam pengelolaan Pihak Ketiga Penyedia Barang/JasaTIK;
b. Hal-hal yang menjadi bagian dalam kontrak/perjanjian kerja sama Pihak Ketiga Penyedia Barang/Jasa TIK dengan DJP;
c. Pengaturan mengenai SLA antara DJP Pihak Ketiga Penyedia Barang/Jasa TIK;

d. Tools untuk membantu pengelolaan Pihak Ketiga Penyedia Barang/JasaTIK;
e. Persyaratan keamanan informasi dalam pengelolaan Pihak Ketiga Penyedia Barang/Jasa TIK; dan
f. Pengaturan mengenai peran dan tanggung jawab pihak-pihak yang terlibat dalam pengelolaan Pihak Ketiga Penyedia Barang/Jasa TIK.

5.3. Pengelolaan Kapasitas Layanan TIK

Kebijakan Pengelolaan Kapasitas Layanan TIK/Capacity Management ini disusun untuk memberikan acuan bagi penyedia Layanan TIK (Direktorat TTKI dan Direktorat TIP) dalam rangka:

a. Memastikan kecukupan kapasitas Layanan TIK sesuai dengan kebutuhan operasional bisnis DJP yang disepakati melalui pembiayaan yang efisien; dan
b. Memastikan kecukupan kapasitas Layanan TIK yang direncanakan akan dilaksanakan di masa yang akan datang.

Kebijakan pengelolaan kapasitas Layanan TIK ini mencakup hal-hal sebagai berikut:

a. Pengaturan dalam perencanaan kapasitas Layanan TIK;
b. Pengaturan dalam pemantauan dan pelaporan kapasitas Layanan TIK;
c. Langkah-langkah dalam optimalisasi kapasitas Layanan TIK;
d. Investasi baru untuk menambah kapasitas Layanan TIK;
e. Pedoman Pengelolaan Kapasitas Layanan TIK; dan
f. Peran dan tanggung jawab pihak-pihak yang terkait dalam pengelolaan kapasitasLayanan TIK.

5.4. Pengelolaan Ketersediaan Layanan TIK

Kebijakan Ketersediaan Layanan TIK/Availability Management ini disusun untuk memberi acuan bagi penyedia Layanan TIK (Direktorat TTKI dan Direktorat TIP) dalam rangka memastikan bahwa tingkat ketersediaan Layanan TIK yang disepakati tercapai.

Kebijakan pengelolaan ketersediaan Layanan TIK ini mencakup hal-hal sebagai berikut:

a. Perencanaan tingkat ketersediaan Layanan TIK;

b. Pengaturan dalam kegiatan operasional yang terkait dengan tingkat ketersediaan Layanan TIK;
c. Pengaturan mengenai penggunaan teknologi dalam memastikan ketersediaan Layanan TIK;
d. Pedoman Pengelolaan Ketersediaan Layanan TIK; dan
e. Pengaturan mengenai peran dan tanggung jawab pihak-pihak yang terkait dalam pengelolaan ketersediaan.

5.5. Service Desk TIK Direktorat Jenderal Pajak

Kebijakan Service Desk TIK DJP ini disusun untuk memberikan acuan kepada penyedia Layanan TIK maupun pengguna Layanan TIK dalam memastikan bahwa permintaan/gangguan/perubahan/informasi terkait Layanan TIK disampaikan, dikelola, dan dipantau dengan baik.

Kebijakan Service Desk TIK DJP ini mencakup hal-hal sebagai berikut:

a. Pengaturan Operasional Service Desk TIK;
b. Ketentuan mengenai Petugas Service DeskTIK; dan
c. Pengaturan mengenai peran dan tanggung jawab pihak-pihak yang terlibat dalamService Desk TIK.

5.6. Pengelolaan Gangguan Layanan TIK

Kebijakan Pengelolaan Gangguan Layanan TIK (*Incident Management*) ini disusun untuk memberi acuan bagi penyedia Layanan TIK dalam memulihkan Layanan TIK ke kondisi normal sesegera mungkin dari gangguan/incident yang dialami oleh pengguna Layanan TIK dengan menerapkan solusi sementara maupun permanen, guna mengurangi kemungkinan hilangnya produktivitas pengguna Layanan TIK. Yang dimaksud dengan gangguan Layanan TIK adalah potensi masalah atau masalah itu sendiri terhadap Layanan TIK, misalnya perangkat TIK tidak dapat bekerja secara normal, Pengguna Layanan TIK gagal dalam mengakses aplikasi, dan lain-lain.

Kebijakan pengelolaan gangguan Layanan TIK ini mencakup hal-hal sebagai berikut:

a. Pengaturan dalam administrasi dan pencatatan gangguan Layanan TIK;
b. Pengaturan dalam penyelesaian gangguan Layanan TIK;

c. Pengaturan dalam Laporan Pengelolaan Gangguan Layanan TIK;
d. Pedoman PengelolaanGangguanLayanan TIK; dan
e. Pengaturan mengenai peran dan tanggung jawab pihak-pihak yang terkait dalam pengelolaan gangguan Layanan TIK.

5.7. **Pengelolaan Problem Layanan TIK**

Kebijakan ini disusun untuk memberi acuan bagi penyedia Layanan TIK dalam rangka melaksanakan pengelolaan problem Layanan TIK (problem management) untuk mengurangi dampak gangguan Layanan TIK dan mencegah terjadinya gangguan Layanan TIK yang berulang dalam rangka menjaga tingkat ketersediaan, tingkat kualitas, dan produktivitas pengguna Layanan TIK. Yang dimaksud dengan problem Layanan TIK adalah permasalahan inti dari satu atau lebih gangguan Layanan TIK yang belum ditemukan solusi sementara atau permanennya, misalnya bug pada aplikasi yang menyebabkan transaksi elektronik sering error.

Kebijakan pengelolaan problem Layanan TIK ini mencakup hal-hal sebagai berikut:

a. Pengaturan dalam penanganan problem Layanan TIK;
b. Evaluasi penanganan problem Layanan TIK;
c. Pedoman Pengelolaan Problem Layanan TIK; dan
d. Pengaturan mengenai peran dan tanggung jawab pihak-pihak yang terkait dalam pengelolaan problem Layanan TIK.

5.8. **Pengelolaan Aset Dan Konfigurasi Layanan TIK**

Kebijakan Pengelolaan Aset dan Konfigurasi Layanan TIK/Configuration Management ini disusun untuk memberi acuan bagi penyedia Layanan TIK (Direktorat TTKI dan Direktorat TIP) dalam memastikan bahwa konfigurasi komponen dan infrastruktur Layanan TIK didefinisikan, diidentifikasi, dikontrol/dikendalikan, dan dikelola dengan baik dalam rangka menyelenggarakan Layanan TIK yang berkualitas secara tepat biaya.

Kebijakan Pengelolaan Aset dan Konfigurasi Layanan TIK ini mencakup hal-hal sebagai berikut:

a. Pengaturan dalam pengelolaan Configuration Management Database (CMDB);
b. Pengaturan mengenai verifikasi aset TIK;
c. Pedoman Pengelolaan Aset dan Konfigurasi Layanan TIK; dan
d. Pengaturan mengenai peran dan tanggung jawab pihak-pihak yang terkait dalam pengelolaan aset dan konfigurasi;

5.9. Pengelolaan Perubahan Layanan TIK

Kebijakan Pengelolaan Perubahan Layanan TIK/Change Management ini disusun dengan tujuan untuk memberikan acuan yang jelas bagi penyedia Layanan TIK (Direktorat TTKI dan Direktorat TIP) dan pengguna Layanan TIK dalam rangka menjamin bahwa perubahan Layanan TIK disampaikan, dianalisis, disetujui, diimplementasikan, dan diawasi dengan baik.

Kebijakan pengelolaan perubahan Layanan TIK ini mencakup hal-hal sebagai berikut:

a. Pengelolaan perubahan Layanan TIK sebagai proses standar dalam melaksanakan perubahan Layanan TIK;
b. Jenis-jenis perubahan Layanan TIK;
c. Pengaturan mengenai permintaan perubahan Layanan TIK;
d. Pengaturan mengenai persetujuan pelaksanaan perubahan Layanan TIK;
e. Pengaturan dalam pelaksanaan/implementasi perubahan Layanan TIK;
f. Pedoman Pengelolaan PerubahanLayanan TIK;
g. Hal-hal mengenai pengelolaan perubahan yang dibahas pada tingkat Tim Pengarah
h. Tata Kelola TIK; dan
i. Pengaturan mengenai peran dan tanggung jawab pihak-pihak yang terkait dalam pengelolaan perubahan.

5.10. Pengelolaan Release Layanan TIK

Kebijakan Pengelolaan Release Layanan TIK ini disusun dengan tujuan untuk menjamin release Layanan TIK yang terjadi pada area operasional diimplementasikan, didistribusikan, dan dapat dilacak dengan baik, tidak

menganggu kualitas Layanan TIK yang telah ada, dan memberikan nilai tambah bagi DJP.

Kebijakan pengelolaan release Layanan TIK ini mencakup hal-hal sebagai berikut:

a. Pengaturan dalam pelaksanaan release Layanan TIK;
b. Kriteria perubahan yang harus dilaksanakan melalui proses release Layanan TIK;
c. Pedoman Pengelolaan Release Layanan TIK;
d. Pengaturan mengenai rollout Layanan TIK; dan
e. Pengaturan mengenai peran dan tanggung jawab pihak-pihak yang terkait dalam pengelolaan release Layanan TIK.

5. Latihan

a. Jelaskan, mengapa tata kelola TIK penting bagi suatu organisasi yang menerapkan TIK !
b. Kebijakan Tata Kelola TIK DJP dijabarkan ke dalam 7 (tujuh) kerangka kerja kebijakan dalam pelaksanaan Tata Kelola TIK DJP. Jelaskan !
c. Jelaskan standar industri yang menjadi acuan dalam menyusun Kebijakan Tata Kelola TIK DJP !
d. Jelaskan tujuan penyusunan Kebijakan Pengelolaan Keamanan Informasi DJP !
e. Jelaskan tujuan penyusunan Kebijakan Pengelolaan Layanan TIK DJP !

6. Rangkuman

Perkembangan teknologi informasi yang demikian pesat, menuntut suatu organisasi untuk mengikutinya. Namun untuk mempersiapkan infrastruktur teknologi informasi ini, ternyata membutuhkan investasi yang tidak sedikit, dan sayang sekali jika investasi teknologi informasi yang cukup besar tersebut, hanya digunakan untuk otomasi pekerjaan, namun sudah saatnya menjadi motor penggerak (*enabler)* terhadap peningkatan kinerja suatu organisasi.

DJP, dalam hal ini telah merumuskan suatu kerangka kerja kebijakan dalam pelaksanaan tata kelola TIK, yang terangkum dalam 7 (tujuh) buku kebijakan Tata Kelola TIK. Kebijakan Tata Kelola TIK DJP ini dibentuk dengan mengacu kepada perangkat hukum yang berlaku, standar industri, dan keperluan internal di DJP

7. Tes Formatif 2

Pilihlah jawaban yang paling tepat !

1. Apa yang dimaksud dengan tata kelola TIK ?
   a) Kumpulan kebijakan, proses dan prosedur untuk mendukung pengoperasian TI
   b) Sekumpulan perangkat TIK yang digunakan dalam suatu institusi/lembaga
   c) Managemen perangkat TIK
   d) Sistem informasi dalam suatu institusi/lembag.

2. Pilihlah pernyataan yang paling tepat terkait pentingnya tata kelola TIK
   a) Investasi TIK Mahal
   b) TIK mengikuti perkembangan jaman
   c) TIK menjadi tuntutan Wajb Pajak untuk pelayanan yang lebih baik
   d) Sebuah instruksi Presiden

3. Pilihlah pernyataan yang tidak tepat terkait tujuan Direktorat Jenderal Pajak mengatur kebijakan tata kelola TIK
   a) Prioritas proyek dan pengadaan TIK sesuai kebutuhan DJP
   b) Pengamanan aset informasi dan penyelenggaraan layanan TIK terkoordinasi
   c) DJP mengikuti perkembangan jaman khususnya terkait TIK
   d) Investasi TIK selaras dengan rencana dan tugas DJP

4. Yang menjadi koordinator pelaksanaan kerangka tata kerja TIK DJP adalah…
   a) Direktur Teknologi dan Informasi Perpajakan
   b) Kepala bidang yang mengelola TIK di setiap Kanwil
   c) Operator Console atau Admin TIK di setiap KPP
   d) Chief Information Officer DJP

5. Untuk mengakses sistem informasi dan aplikasi DJP lainnya, DJP sudah menerapkan sistem…

a) Single Sign On
b) Joint Domain
c) Direct Access
d) Proxy Gateway

6. Pedoman untuk pengelolaan aset informasi, diatur dalam kebijakan terkait Pengelolaan…
   a) Layanan TIK
   b) Keamanan informasi TIK
   c) Proyek TIK
   d) Pengadaan aset TIK

7. Adanya Lasis Online merupakan produk nyata dari kebijakan tata kelola TIK, khususnya terkait Pengelolaan…
   a) Pengembangan TIK
   b) Layanan TIK
   c) Keamanan informasi TIK
   d) Proyek TIK

8. Pengembangan aplikasi oleh unit kerja pengguna, diperkenankan dengan ketentuan …
   a) Aplikasi boleh mengubah master data utama
   b) Aplikasi boleh mengubah hanya master data local
   c) Aplikasi hanya bersifat analitis
   d) Aplikasi hanya bersifat deskriptif

9. Untuk memastikan TIK berlangsung dalam jangka panjang, apakah yang sudah dilakukan DJP …
   a) Membangun disaster recovery center di suatu tempat tertentu
   b) Melakukan sentralisasi sistem informasi di Kantor Pusat DJP
   c) Melakukan desentralisasi sistem informasi di setiap Kanwil DJP
   d) Melakukan desentralisasi sistem informasi di setiap KPP

10. Monitoring dan Evaluasi TIK DJP dilakukan oleh…

a) Unit TIK DJP
b) Chief Information Officer
c) Chief Operating Officer
d) Sub Direktorat Analisis dan Evaluasi Sistem Informasi

8. Umpan Balik dan Tindak Lanjut

Cocokanlah jawaban anda dengan kunci jawaban Tes Formatif 2 yang terdapat di bagian akhir modul ini. Hitunglah jawaban yang benar.

Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaaan anda terhadap materi Kegiatan Belajar 2.

$$\text{Tingkat penguasaan} = \frac{\text{Jumlah Jawaban yang Benar}}{\text{Jumlah Soal}} \times 100\ \%$$

Arti tingkat penguasaan	=	90 – 100%	= Baik Sekali
		80 – 89 %	= Baik
		70 – 79 %	= Cukup
		< 70 %	= Kurang

Penjelasan:

PENGETAHUAN ORGANISASI DAN TATA LAKSANA ORGANISASI TIK DJP

1. Indikator

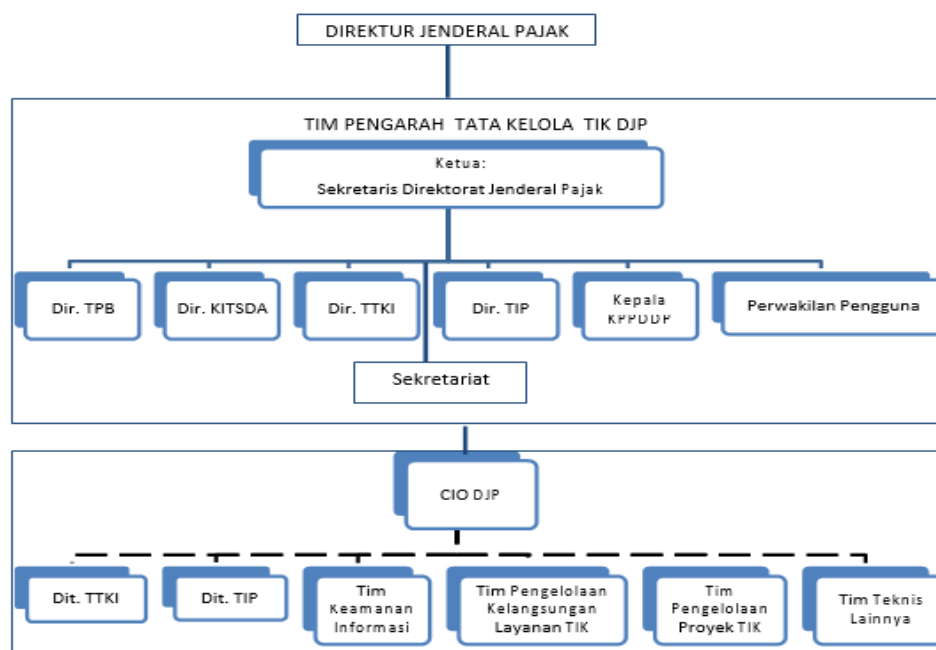
Setelah mengikuti pembelajaran, peserta diklat mampu :

☑ memahami struktur organisasi TIK DJP

☑ memahami proses bisnis TIK DJP

2. Organisasi TIK DJP

Struktur organisasi penyelenggaraan Tata Kelola TIK DJP dapat dilihat pada diagram berikut:

Gambar 3.1 Struktur Organisasi TIK DJP

Untuk memastikan terselenggaranya Tata Kelola TIK DJP secara bertahap dan berkesinambungan, maka Direktur Jenderal Pajak berwenang menunjuk Tim Pengarah Tata Kelola TIK DJP dan CIO DJP.

Tim Pengarah Tata Kelola TIK DJP ditetapkan oleh Direktur Jenderal Pajak, diketuai oleh Sekretaris Direktorat Jenderal Pajak dan beranggotakan Direktur Transformasi Proses Bisnis, Direktur Kepatuhan Internal dan Transformasi Sumber Daya Aparatur, Direktur Transformasi Teknologi Komunikasi dan Informasi, Direktur Teknologi Informasi Perpajakan, Kepala Pusat Pengolahan Data dan Dokumen Perpajakan, serta perwakilan pengguna dari Kantor Wilayah DJP dan Kantor Pelayanan Pajak.

Tugas Tim Pengarah Tata Kelola TIK DJP adalah memberikan arahan/rekomendasi dalam penyelenggaraan Tata Kelola TIK DJP dan mengawasi kinerja penerapan teknis oleh CIO DJP dan unit kerja TIK maupun tim fungsional/teknis yang dibentuk sesuai dengan keperluan masing-masing area pengelolaan TIK

Direktur Jenderal Pajak juga menunjuk seorang Chief Information Officer Direktorat Jenderal Pajak (CIO DJP) untuk mengkoordinasikan seluruh kegiatan TIK agar dapat berjalan secara harmonis dalam mendukung visi, misi, dan rencana strategis DJP. CIO DJP ini merupakan pejabat eselon II yang memimpin unit kerja TIK Direktorat Jenderal Pajak, yang bertugas untuk mengkoordinasikan perencanaan, penerapan, dan peningkatan efektivitas pelaksanaan kegiatan Tata Kelola TIK DJP.

Penerapan Tata Kelola TIK secara prinsip akan menjadi tanggung jawab Tim Pengarah Tata Kelola TIK DJP yang dibentuk sebagai representasi kepemimpinan DJP untuk aspek pengelolaan TIK dan pelaksanaan teknisnya dikoordinasikan oleh unit kerja TIK DJP, yang dalam hal ini adalah Direktorat Teknologi Informasi Perpajakan (TIP) dan Direktorat Transformasi Teknologi Komunikasi dan Informasi (TTKI).

yang mencakup layanan TIK, pengelolaan keamanan informasi, pelaksanaan kelangsungan layanan TIK, pengelolaan proyek dan pengembangan TIK, dan evaluasi kinerja TIK dilaporkan secara berkala dari Unit Kerja TIK kepada Tim Pengarah Tata Kelola TIK DJP melalui CIO DJP.

Dalam struktur TIK DJP juga terdapat beberapa tim yang dibentuk oleh Direktur Jenderal Pajak, yaitu Tim Keamanan Informasi yang bertugas memelihara

dan mengontrol penerapan keamanan informasi di DJP; Tim Pengelolaan kelangsungan layanan TIK untuk bertugas untuk mengelola kelangsungan layanan TIK bagi kepentingan layanan proses perpajakan di DJP; Tim Pengelolaan Proyek TIK yaitu tim yang terdiri dari pegawai DJP yang ditunjuk untuk melaksanakan dan menyelesaikan kegiatan proyek TIK; dan tim teknis lainnya sesuai yang dibutuhkan.

3. Proses Bisnis TIK

Untuk mendukung jalannya proses bisnis utamanya, DJP menyediakan TIK dalam bentuk Sistem Informasi DJP (SIDJP) dan *help desk* (layanan bantuan teknis) terkait. Untuk pengambilan keputusan, khususnya keputusan-keputusan strategis, DJP juga memanfaatkan aplikasi dashboard & reporting.

Selain itu, DJP juga menyediakan aplikasi pendukung seperti Approweb, Aplikasi Portal DJP, dan aplikasi-aplikasi pendukung lainnya untuk kebutuhan-kebutuhan tertentu. Aplikasi-aplikasi tersebut mengadopsi arsitektur client-server yang berbasis Web sehingga dapat diakses lewat infrastruktur jaringan komunikasi internal DJP.

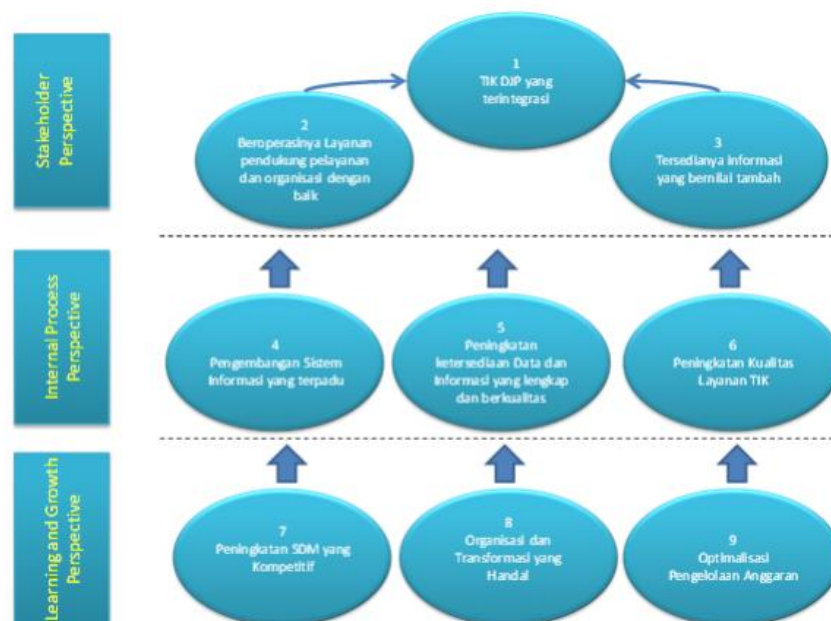
Infrastruktur yang dimiliki DJP meliputi jaringan komunikasi data skala nasional yang menggunakan fiber optic, data center (pusat data), dan disaster recovery center (pusat pemulihan bencana).

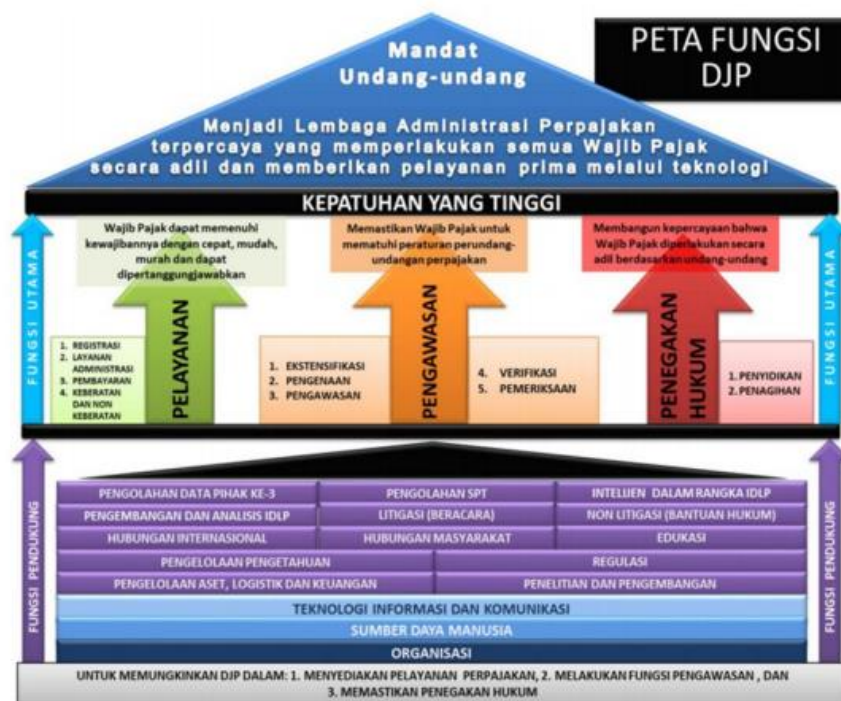
Sementara itu, unit kerja yang memiliki fungsi pengembangan dan fungsi operasional TI di DJP mencakup 2 unit eselon II di Kantor Pusat DJP, yaitu Direktorat Teknologi Informasi Perpajakan (TIP) dan Direktorat Transformasi Teknologi Komunikasi dan Informasi (TTKI), Unit Pengolahan Data dan Dokumen Perpajakan yang terdiri dari 1 unit setingkat eselon IIb, yaitu Pusat Pengolahan Data dan Dokumen Perpajakan (PPDDP) dan 2 unit setingkat eselon IIIb, yaitu Kantor Pengolahan Data dan Dokumen Perpajakan (KPDDP), 1 unit setingkat eselon IIIb, yaitu Kantor Pengolahan Data Eksternal (KPDE), 1 unit eselon III di masing-masing kantor wilayah (kanwil), dan 1 unit eselon IV di masing-masing kantor pelayanan pajak (KPP). Unit eselon IV di masing-masing KPP itu juga memberikan dukungan teknis kepada kantor pelayanan, penyuluhan, dan konsultasi perpajakan (KP2KP) yang ada di dalam wilayahnya.

Seiring dengan diresmikannya Rencana Strategis DJP tahun 2015-2019 melalui Keputusan Direktur Jenderal Pajak Nomor 95/PJ/2015 tanggal 27 April

2015, DJP perlu menyusun kembali rencana strategis di bidang TIK agar sumber daya TIK yang dimiliki dapat mendukung pelaksanaan inisiatif strategis DJP sehingga TIK dapat menjadi motor penggerak DJP dengan memanfaatkan tren dan teknologi terkini secara optimal untuk mencapai sasaran-sasaran strategis DJP.

Untuk menjadikan TIK sebagai motor penggerak, DJP harus mengikuti tren di bidang TIK, khususnya yang terkait dengan Internet. Seperti kita ketahui, akses Internet saat ini tidak lagi terbatas pada komputer (PC), baik desktop maupun laptop, tapi sudah meluas ke perangkat-perangkat mobile mulai dari smartphone sampai tablet. Penggunaan wearable dan tren Internet of Things (IoT) juga terus meningkat sehingga Internet semakin terintegrasi ke dalam berbagai sisi kehidupan. Tingginya pemanfaatan Internet tersebut mendorong terwujudnya limpahan data di Internet yang menjadi salah satu sumber big data. Big Data analytics digunakan untuk mempelajari pola di dalam big data yang dapat dimanfaatkan untuk mengenal lebih dekat klien-klien mereka. Semua tren tersebut serta kemajuan TIK di masa depan akan menjadi bahan pertimbangan dalam menyusun dan meninjau kembali rencana strategis DJP di bidang TIK. Berikut adalah Rencana Strategis TIK DJP 2015-2019.

Gambar 3.2 Rencana Strategis TIK DJP 2015-2019

DJP, melalui Unit Kerja TIK, perlu menyediakan layanan TIK, baik untuk pengguna internal (pegawai DJP) maupun untuk pengguna eksternal (WP dan pihak eksternal lainnya), untuk menjalankan fungsinya. Fungsi DJP tersebut dapat dibagi 2 (dua) kategori, yaitu fungsi utama dan fungsi pendukung. Fungsi utama DJP adalah pelayanan, pengawasan, dan penegakan hukum, sementara fungsi pendukung DJP terdiri dari sejumlah aktivitas yang berfungsi untuk mendukung terlaksananya fungsi-fungsi utama tersebut.

Gambar 3.3 Peta Fungsi DJP

Berdasarkan peta fungsi DJP di atas, TIK menjadi salah satu fungsi pendukung yang berperan penting untuk mencapai tujuan organisasi. Wujud nyata Unit TIK dalam mendukung tercapainya visi misi DJP adalah dengan memberikan layanan-layanan TIK sebagai berikut:

1. Layanan Sistem Informasi Administrasi Perpajakan;
2. Layanan Sistem Informasi Pendukung Organisasi;
3. Layanan terkait Stakeholder;
4. Layanan Analisis Data;
5. Layanan Dukungan Teknis TIK.

3.1. Layanan Sistem Informasi Administrasi Perpajakan

Layanan ini diharapkan dapat memenuhi kebutuhan DJP untuk menjalankan fungsi utamanya. Masing-masing fungsi utama tersebut didukung oleh proses-proses bisnis tertentu agar fungsi terkait dapat berjalan dengan baik. Berbagai proses bisnis yang terkait dengan fungsi-fungsi utama DJP adalah sebagai berikut:

1) Fungsi Pelayanan.

Proses bisnis dalam fungsi Pelayanan yaitu:

i. Registrasi.

Proses Bisnis Registrasi merupakan aktivitas yang paling awal dilakukan dalam proses administrasi perpajakan. Proses Bisnis Registrasi adalah proses pemberian identitas dan pemutakhiran data identitas WP (NPWP) dan/atau pengukuhan Pengusaha Kena Pajak (PKP) dalam rangka pembentukan dan pemutakhiran data perpajakan.

ii. Layanan Administrasi.

Proses Bisnis Layanan Administrasi adalah kelompok proses bisnis yang menggambarkan aktivitas-aktivitas atau rangkaian aktivitas dalam rangka pemberian layanan kepada WP sebagai bagian dari haknya setelah mendaftarkan dirinya menjadi WP dan pemberian layanan kepada non-WP.

iii. Pembayaran.

Proses Bisnis Pembayaran merupakan kelompok proses bisnis yang menggambarkan rangkaian siklus pembayaran pajak, mulai dari penerimaan data pembayaran pajak, penyesuaian atas pengakuan penerimaan pajak, serta pelaporan penerimaan pajak.

iv. Keberatan.

Proses Keberatan terdiri atas Proses Keberatan menurut Pasal 25 UU KUP dan Keberatan Pajak Bumi dan Bangunan (PBB) menurut Pasal 15 UU PBB. Proses Keberatan (Pasal 25 UU KUP) adalah proses penyelesaian sengketa antara WP dan fiskus apabila WP merasa tidak sependapat atas suatu ketetapan pajak atau atas pemotongan/pemungutan pajak oleh pihak ketiga yang dikenakan kepadanya. Keberatan PBB (Pasal 15 UU PBB) adalah proses penyelesaian sengketa antara WP dan fiskus apabila WP merasa tidak

sependapat atas luas objek pajak bumi dan/atau bangunan atau nilai jual objek pajak bumi dan/atau bangunan, atau penafsiran peraturan perundang-undangan PBB yang mengakibatkan perbedaan jumlah PBB terutang.

v. Non Keberatan.

Kelompok Proses Bisnis Non Keberatan adalah kelompok proses bisnis yang menggambarkan rangkaian aktivitas dalam rangka penerimaan permohonan non keberatan, pembuatan usulan secara jabatan, persiapan pelaksanaan penelitian, pelaksanaan penelitian dan evaluasi atas Surat Keputusan. Kelompok proses bisnis ini meliputi penyelesaian proses bisnis Non Keberatan yang mencakup Pembetulan (diatur dalam Pasal 16 UU KUP), Pengurangan – Penghapusan – Pembatalan (diatur dalam Pasal 36 ayat (1) UU KUP dan Pasal 19 UU PBB).

2) Fungsi Pengawasan

Proses bisnis dalam fungsi Pengawasan yaitu:

i. Ekstensifikasi.

Proses Bisnis Ekstensifikasi adalah kelompok proses bisnis yang menggambarkan rangkaian aktivitas dalam rangka pemberian Nomor Pokok Wajib Pajak (NPWP) dan/atau pengukuhan Pengusaha Kena Pajak (PKP).

ii. Pengawasan.

Proses Bisnis Pengawasan adalah kelompok proses bisnis yang menggambarkan aktivitas-aktivitas atau rangkaian aktivitas dalam rangka mewujudkan pemahaman dan kesadaran pajak WP melalui pengawasan kepatuhan WP. Pada proses ini tujuan yang akan dicapai adalah terciptanya pemahaman WP atas kewajiban perpajakannya sehingga terwujud WP yang patuh melalui sistem pengawasan WP yang baik dan terpadu.

iii. Pemeriksaan.

Proses Bisnis Pemeriksaan adalah serangkaian kegiatan menghimpun dan mengolah data, keterangan, dan/atau bukti yang dilaksanakan secara objektif dan profesional berdasarkan suatu standar pemeriksaan untuk menguji kepatuhan pemenuhan kewajiban perpajakan

dan/atau untuk tujuan lain dalam rangka melaksanakan ketentuan peraturan perundang-undangan perpajakan.

iv. Pengenaan.

Proses Bisnis Pengenaan merupakan serangkaian kegiatan untuk menetapkan WP PBB (Pajak Bumi dan Bangunan) dan menentukan besarnya PBB terutang berdasarkan ketentuan peraturan perundang-undangan.

3) Fungsi Penegakan Hukum.

Proses bisnis dalam fungsi Penegakan Hukum yaitu:

i. Penyidikan.

Proses Bisnis Penyidikan adalah proses bisnis yang menggambarkan serangkaian aktivitas untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tindak pidana di bidang perpajakan, menggambarkan apa yang terjadi dan menemukan tersangkanya, serta mengetahui besarnya kerugian negara. Penyidikan dilaksanakan oleh Tim Penyidik Pajak yang terdiri dari para penyidik pajak pada Kantor Pusat DJP dan/atau para penyidik pada kantor wilayah DJP.

ii. Penagihan.

Proses Bisnis Penagihan adalah proses bisnis yang menggambarkan serangkaian tindakan agar Penanggung Pajak melunasi utang pajak dan biaya penagihan pajak dengan menegur atau mengingatkan, melaksanakan penagihan seketika dan sekaligus, memberitahukan Surat Paksa, mengusulkan pencegahan, melaksanakan penyitaan, melaksanakan penyanderaan, melakukan lelang terhadap barang yang telah disita, termasuk didalamnya penatausahaan dan penghapusan piutang pajak.

3.2. Layanan Sistem Informasi Pendukung Organisasi

Layanan ini diharapkan dapat memenuhi kebutuhan DJP untuk menjalankan fungsi pendukung DJP. Fungsi pendukung DJP tersebut terdiri dari 12 proses bisnis, yaitu:

1) Pengolahan SPT;

2) Intelijen dalam rangka informasi, data, laporan, dan pengaduan (IDLP);
3) Pengembangan dan Analisis IDLP;
4) Litigasi (Beracara);
5) Hubungan Masyarakat;
6) Edukasi;
7) Non Litigasi (Bantuan Hukum);
8) Hubungan Internasional;
9) Pengelolaan Pengetahuan;
10) Regulasi;
11) Pengelolaan Aset, Logistik, dan Keuangan;
12) Penelitian dan Pengembangan. Penjelasan rinci mengenai masing-masing proses bisnis di atas dapat ditemukan dalam Peta Fungsi DJP versi 1.1 Tahun 2015.

3.3. Layanan terkait Stakeholders

Layanan ini diharapkan dapat menghubungkan DJP dengan stakeholders/mitra DJP yaitu: WP, Bank, Kementerian atau Badan Pemerintahan lainnya. Layanan ini juga diharapkan dapat menyediakan saluran untuk pertukaran data dan informasi dan juga sebagai media publikasi informasi dari DJP ke mitra DJP. Layanan ini juga diharapkan dapat memenuhi kebutuhan salah satu fungsi pendukung DJP yaitu Pengolahan Data Pihak Ketiga. Proses Bisnis Pengolahan Data Pihak Ketiga merupakan proses bisnis yang menggambarkan kegiatan pengumpulan data kegiatan usaha WP yang diperoleh dari sumber data selain laporan WP itu sendiri, seperti dari instansi pemerintah, lembaga, asosiasi, dan pihak lain (ILAP) yang wajib memberikan data dan informasi terkait perpajakan kepada DJP sebagaimana dimaksud dalam Pasal 35A Undang Undang KUP.

3.4. Layanan Analisis Data

Layanan ini diharapkan dapat menyediakan hasil olahan data dan informasi yang dapat digunakan untuk pimpinan DJP dalam mengambil keputusan.

3.5. Layanan Dukungan Teknis TIK

Layanan ini diharapkan dapat menghubungkan unit kerja di DJP dengan unit TIK DJP. Setiap permasalahan, pertanyaan, ataupun permintaan seputar TIK disampaikan melalui satu pintu.

4. Latihan

a. Jelaskan Struktur organisasi TIK DJP !
b. Jelaskan tugas dari Tim Pengarah TIK dan tugas seorang Chief Information Officer !
c. Jelaskan Rencana Strategis TIK DJP 2015-2019 !
d. Jelaskan bentuk-bentuk layanan TIK DJP !
e. Jelaskan peran TIK terkait fungsi DJP!

5. Rangkuman

Berdasarkan Rencana Strategis DJP tahun 2015-2019 disusun rencana strategis di bidang TIK agar sumber daya TIK yang dimiliki dapat mendukung pelaksanaan inisiatif strategis DJP sehingga TIK dapat menjadi motor penggerak DJP untuk mencapai sasaran-sasaran strategis DJP. Terdapat tiga perspektif dalam rencana strategis TIK ini, yaitu stakeholder perspective, internal process perspective dan learning and growth Perspective, namun secara umum dapat digolongkan dalam penyediaan layanan TIK untuk pengguna internal (pegawai DJP) dan untuk pengguna eksternal (WP dan pihak eksternal lainnya) untuk menjalankan fungsinya masing-masing. Penyediaan layanan TIK ini secara teknis dikoordinasikan oleh unit kerja TIK DJP, yang dalam hal ini adalah Direktorat Teknologi Informasi Perpajakan (TIP) dan Direktorat Transformasi Teknologi Komunikasi dan Informasi (TTKI).

6. Tes Formatif 3

Pilihlah jawaban yang paling tepat !

1. Yang tidak termasuk Tim Pengarah Tata Kelola TIK DJP adalah…
   a) Direktur Transformasi Proses Bisnis,
   b) Direktur Kepatuhan Internal dan Transformasi Sumber Daya Aparatur
   c) Kepala Pusat Pengolahan Data dan Dokumen Perpajakan
   d) Direktur Peraturan Perpajakan I

2. Unit kerja TIK DJP adalah…

a) TTKI dan TIP
b) TTKI
c) TIP
d) Chief Information Officer (CIO)

3. Yang bertugas untuk mengkoordinasikan perencanaan, penerapan, dan peningkatan efektivitas pelaksanaan kegiatan Tata Kelola TIK DJP adalah…
   a) TTKI dan TIP
   b) TTKI
   c) TIP
   d) Chief Information Officer (CIO)

4. Mengawasi kinerja penerapan teknis oleh CIO DJP dan unit kerja TIK maupun tim fungsional/teknis yang dibentuk sesuai dengan keperluan masing-masing area pengelolaan TIK adalah tugas …
   a) Tim Pengarah Tata KeLola TIK
   b) Tim Pengawas Tata KeLola TIK
   c) Direktur TIP
   d) Sekretaris Ditjen Pajak

5. Dalam Peta Fungsi DJP, yang tidak termasuk fungsi utama DJP adalah …
   a) Pelayanan
   b) Penyuluhan
   c) Pengawasan
   d) Penegakan Hukum

6. Aktivitas yang paling awal dilakukan dalam proses administrasi perpajakan didukung oleh suatu proses bisnis …
   a) Penyuluhan
   b) Registrasi
   c) Pembayaran
   d) Pelaporan

7. Kelompok proses bisnis yang menggambarkan aktivitas-aktivitas atau rangkaian aktivitas dalam rangka pemberian layanan kepada WP sebagai bagian dari haknya setelah mendaftarkan dirinya menjadi WP dan pemberian layanan kepada non-WP …
   a) Proses Bisnis Pelayanan
   b) Proses Bisnis Registrasi
   c) Proses Bisnis Layanan Administrasi
   d) Proses Bisnis Pengawasan

8. Yang tidak termasuk proses bisnis dalam fungsi Pengawasan adalah…
   a) Ekstensifikasi
   b) Penagihan

c) Pemeriksaan
   d) Pengenaan

9. Yang termasuk proses bisnis dalam fungsi penegakan hukum adalah…
   a) Pemeriksaan
   b) Penagihan
   c) Bukti Permulaan
   d) Himbauan

10. Layanan yang dapat menyediakan hasil olahan data dan informasi yang dapat digunakan untuk pimpinan DJP dalam mengambil keputusan adalah layanan …
    a) Dukungan Teknis Perpajakan
    b) Analisis Data
    c) Supporting Data
    d) Sistem informasi pendukung

7. Umpan Balik dan Tindak Lanjut

Cocokanlah jawaban anda dengan kunci jawaban Tes Formatif 2 yang terdapat di bagian akhir modul ini. Hitunglah jawaban yang benar.

Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaaan anda terhadap materi Kegiatan Belajar 2.

$$\text{Tingkat penguasaan} = \frac{\text{Jumlah Jawaban yang Benar}}{\text{Jumlah Soal}} \times 100\ \%$$

Arti tingkat penguasaan	=	90 – 100%	= Baik Sekali
		80 – 89 %	= Baik
		70 – 79 %	= Cukup
		< 70 %	= Kurang

Penjelasan:

PENUTUP

Setelah mempelajari modul ini, diharapkan peserta dapat menggunakan pengetahuan yang terdapat dalam modul ini untuk tujuan pencarian data dalam proses penagihan pajak.

Selanjutnya lakukan pengujian secara komprehensif terhadap seluruh Kegiatan Belajar dalam modul ini, agar diketahui tingkat pemahaman peserta dalam memahami modul ini.

Pengujian dilakukan dengan cara menjawab soal-soal Latihan, Tes Formatif dan Tes Sumatif, kemudian cocokanlah jawaban anda dengan kunci jawaban Tes Formatif dan Sumatif yang terdapat di bagian akhir modul ini. Hitunglah jawaban yang benar, kemudian gunakan rumus berikut untuk mengetahui tingkat penguasaaan peserta terhadap materi kegiatan belajar di modul ini.

$$\text{Tingkat penguasaan} = \frac{\text{Jumlah Jawaban yang Benar}}{\text{Jumlah Soal}} \times 100\,\%$$

Arti tingkat penguasaan =

Arti tingkat penguasaan =	90 – 100%	= Baik Sekali
	80 – 89 %	= Baik
	70 – 79 %	= Cukup
	< 70 %	= Kurang

Apabila mencapai tingkat penguasaan 80% atau lebih, Peserta dapat dinyatakan sudah menguasai modul ini.Jika masih di bawah 80%**,** Peserta harus mengulangi materi Kegiatan Belajar, terutama bagian Kegiatan Belajar yang belum dikuasai.

TES SUMATIF

Pilihlah jawaban yang paling tepat !

1. CBTIK DJP 2015-2019 disusun sedemikian rupa untuk mencapai tujuan-tujuan tertentu. Salah satu tujuannya adalah …
   a) Menjadi acuan melaksanakan proyek seluruh kegiatan yang berhubungan dengan TIK di DJP
   b) Menjadi acuan bagi semua sumber daya manusia DJP dalam memahami TIK DJP
   c) Menjadi acuan perencanaan sumber daya yang diperlukan untuk melaksanakan seluruh kegiatan TIK di DJP
   d) Menjadi acuan dalam mengikuti perkembangan jaman yang mengarah kepada penggunaan TIK

2. Pengembangan TIK di DJP diarahkan untuk mendukung terwujudnya layanan kepada WP yang tidak dibatasi ruang dan waktu. Pernyataan tersebut adalah prinsip pilar pengembangan TIK…
   a) *Social Business*
   b) *Mobility*
   c) *Cloud Computing*
   d) *Statistics*

3. Beragamnya jenis data dan struktur data akan dapat menyebabkan pola dan korelasi antar data sulit untuk digambarkan. Untuk itu DJP mengembangkan aplikasi yang memanfaatkan teknologi…
   a) *Data Analytics*
   b) *Mobility Business*
   c) *Cloud Computing*
   d) *Big Data*

4. Aplikasi-aplikasi yang dapat mengubah arah kebijakan dan kegiatan operasional di dalam lingkungan DJP dengan tujuan untuk mengoptimalkan penerimaan pajak termasuk dalam kuadran …

a) High Potential
b) Strategic
c) Key Operational
d) Support

5. Aplikasi-aplikasi yang harus ada (*mandatory*) untuk menjalankan proses bisnis utama di dalam lingkungan DJP secara efektif dan efisien termasuk dalam kuadran …
   a) High Potential
   b) Strategic
   c) Key Operational
   d) Support

6. Tata Kelola TIK DJP disusun menjadi 7 (tujuh) buku dengan format penyusunan yang dibagi berdasarkan …
   a) Tujuan
   b) Fungsi
   c) Manfaat
   d) Jabatan

7. Kerangka kerja kebijakan dalam pelaksanaan Tata Kelola TIK DJP yang tercantum dalam Buku 2 adalah terkait …
   a) Kebijakan Tata Kelola TIK DJP
   b) Kebijakan Pengelolaan Keamanan Informasi
   c) Kebijakan Pengelolaan Layanan TIK
   d) Kebijakan Pengembangan TIK

8. Kerangka kerja kebijakan dalam pelaksanaan Tata Kelola TIK DJP yang tercantum dalam Buku 3 adalah terkait …
   a) Kebijakan Tata Kelola TIK DJP
   b) Kebijakan Pengelolaan Keamanan Informasi
   c) Kebijakan Pengelolaan Layanan TIK
   d) Kebijakan Pengembangan TIK

9. Kebijakan Tata Kelola TIK DJP ini dibentuk dengan mengacu kepada …
   a) instruksi Direktur Jenderal, kebutuhan TIK dan standar industri
   b) kebutuhan TIK, standar industri, dan instruksi Direktur Jenderal
   c) perangkat hukum yang berlaku, standar industri, dan keperluan internal di DJP
   d) proses bisnis, standar industri, dan keperluan internal di DJP

10. Berikut ini adalah yang tidak termasuk tujuan disusunnya Kebijakan Pengelolaan Keamanan Informasi DJP …
    a) Mendukung DJP dalam mencapai salah satu sasarannya yaitu melaksanakan modernisasi di bidang teknologi informasi dan komunikasi
    b) Menyediakan perangkat pengaturan dalam pengelolaan keamanan informasi
    c) Menyediakan perangkat yang digunakan oleh pimpinan untuk melakukan monitoring sistem informasi
    d) Melindungi kerahasiaan, keutuhan, dan ketersediaan aset informasi DJP dari segala bentuk gangguan dan ancaman baik dari dalam maupun luar DJP, yang dilakukan secara sengaja atau tidak.

11. Kebijakan DJP, panduan kerja, tata cara kerja, instruksi kerja, memo/publikasi internal, informasi yang disediakan dalam intranet, dan data operasional IT lainnya adalah contoh dari aset informasi yang bersifat…
    a) Sangat Rahasia
    b) Rahasia
    c) Terbatas
    d) Publik

12. *IP address* dan *password* komputer masing-masing pegawai DJP adalah contoh dari aset informasi yang bersifat…
    a) Sangat Rahasia
    b) Rahasia
    c) Terbatas

d) Publik

13. Berikut ini adalah kegiatan yang diijinkan bagi pemilik *user account* …
    a) Memberitahukan *password*nya kepada siapa pun
    b) Menggunakan fasilitas *remember password* untuk mengakses aset TIK DJP
    c) Mengganti password secara berkala
    d) Menggunakan password yang sama antara fasilitas TIK DJP dengan di luar fasilitas DJP

14. Berikut ini adalah materi yang tidak diatur dalam Buku 3 Tata Kelola TIK DJP…
    a) Service Desk TIK
    b) Pengelolaan gangguan layanan TIK
    c) Pengelolaan layanan peminjaman data
    d) Pengelolaan Pihak Ketiga Penyedia Barang/Jasa TIK

15. Penyelenggaraan Tata Kelola TIK dan Evaluasi Kinerja TIK dilaporkan oleh CIO kepada …
    a) Tim Pengarah Tata KeLola TIK
    b) Tim Pengawas Tata KeLola TIK
    c) Direktur Jenderal Pajak
    d) Sekretaris Ditjen Pajak

JAWABAN TEST

TES FORMATIF 1

1. C	6. D
3. D	7. C
4. A	8. D
4. C	9. D
5. A	10. C

TES FORMATIF 2

1. A	6. B
2. A	7. B
3. C	8. C
4. D	9. A
5. A	10. A

TES FORMATIF 3

1. D	6.
2. A	7.
3. D	8.
4. B	9.
5.	10.

TES SUMATIF

1. C	6. B	11. C
2. B	7. B	12. B
3. D	8. C	13. C
4. B	6. C	14. C
5. C	10. C	15. A

REFERENSI

Grewal, Peter and Knutsson, Fredrik, 2005, *It Governance In A Global Logistics Company*, Göteborg University And Chalmers University Of Technology Göteborg, Sweden.

Keputusan Direktur Jenderal Pajak Nomor 95/PJ/2015 tanggal 27 April 2015 tentang Rencana Strategis DJP tahun 2015-2019.

Peraturan Direktur Jenderal Pajak Nomor PER-46/PJ/2015 Tentang Cetak Biru Teknologi Informasi dan Komunikasi Direktorat Jenderal Pajak Tahun 2015-2019.

Peraturan Direktur Jenderal Pajak Nomor PER - 37/PJ/2010 Tentang Kebijakan Tata Kelola Teknologi Informasi Dan Komunikasi Direktorat Jenderal Pajak

Peraturan Direktur Jenderal Pajak Nomor PER - 41/PJ/2010 Tentang Kebijakan Pengelolaan Keamanan Informasi Direktorat Jenderal Pajak

Peraturan Direktur Jenderal Pajak Nomor Per- 50 /PJ/2010 Tentang Kebijakan Pengelolaan Layanan Teknologi Informasi Dan Komunikasi Direktorat Jenderal Pajak

Putra, Risma Bayu dan Sensuse, Dana Indra, 2008, *Rancangan Tata Kelola TI untuk Institusi Pemerintah Studi Kasus Bappenas*, Jurnal Sistem Informasi MTI-UI, Volume 4, Nomor 1.